НАХОДКА ДЛЯ СПЕЦИАЛИСТА!

«РЕМОНТ» № 93

С. А. Сотников

Программный ремонт сотовых телефонов

– Более 200 моделей 1995-2005 г.г. выпуска

LG
MOTOROLA
NOKIA
SIEMENS

– Методики разблокировки и прошивки ПО
– Принципиальные схемы DATA-кабелей

БОНУС:
Описание и схемы универсальных боксов

РЕМОНТ & СЕРВИС

УДК 621.396.218
ББК 32.884.1
С 67

Серия «Ремонт», выпуск 93

Приложение к журналу «Ремонт & Сервис»

С. А. Сотников / Под общей редакцией А. В. Родина и Н. А. Тюнина.

Программный ремонт сотовых телефонов. — М.: СОЛОН-ПРЕСС, 2006. — 96 с.: ил. (Серия «Ремонт», выпуск 93).

ISBN 5-90219-719-8

Предлагаемая книга является уникальной в своем роде — аналогов ей пока нет не только в России, но и в странах СНГ и Балтии. В пособии собраны материалы по программированию более 200 моделей сотовых телефонов торговых марок SIEMENS, MOTOROLA, NOKIA и LG.

Кроме описания методики программирования телефонов с помощью наиболее распространенных программных средств, в книге приводятся схемы интерфейсных кабелей (DATA-кабелей), различных видов программаторов-боксов, а также назначение выводов системных разъемов телефонов.

Для некоторых моделей приводятся описания тестовых режимов, рассматриваются характерные дефекты аппаратов и их устранение.

В книге приводятся все необходимые начальные сведения по архитектуре рассматриваемых моделей телефонов, распределению их памяти и другим аппаратным особенностям Благодаря этому, она может использоваться в качестве учебного пособия при подготовке специалистов по ремонту сотовых телефонов.

При подготовке книги использовались материалы журнала «Ремонт & Сервис» за 2004—2006 гг.

Сайт издательства «Ремонт и Сервис 21»: www.remserv.ru
Сайт издательства «СОЛОН-ПРЕСС»: www.solon-press.ru

ISBN 5-90219-719-8

Предисловие

Предлагаемая книга является **первой** и **единственной** в настоящее время публикацией в России по программированию сотовых телефонов, а также ремонту их программной начинки. В ней приведены материалы по программированию большинства распространенных в России моделей сотовых телефонов торговых марок SIEMENS, MOTOROLA, NOKIA и LG (*всего более 200 моделей*).

Известно, что большинство неисправностей сотовых телефонов происходят по двум основным причинам:

— различные механические или электрические повреждения, повлекшие за собой отказ тех или иных узлов телефона;
— неисправности, вызванные сбоями в работе программного обеспечения, «прошитого» в микросхеме FLASH-памяти телефона.

В первом случае порядок восстановления работоспособности телефона достаточно ясен — исходя из алгоритмов проверки, которые приводятся в сервисной документации, проверяется работоспособность его узлов и определяется неисправный элемент.

Во втором случае все несколько сложнее, потому что **информация по устранению дефектов телефонов, связанных со сбоями программного обеспечения до сих пор нигде не публиковалась**.

Сложность диагностики заключается в том, что многие дефекты телефонов, связанные с проблемами их программного обеспечения, внешне проявляются как чисто аппаратные неисправности Есть попытки развить эту тему в Интернете, но большинство представленных сегодня материалов не систематизированы и не могут похвастаться полнотой.

К сожалению, **в таких сведениях зачастую встречаются неточные или даже ошибочные данные, использование которых может вывести из строя аппаратную часть телефона**. Некоторым утешением служит лишь то, что не все специалисты-ремонтники с доверием относятся к подобного рода материалам, так как уже не раз сталкивались на практике с негативными последствиями неосторожного заимствования чужих «опытов» по ремонту технически сложных аппаратов, которыми являются современные телефоны.

Для всех рассматриваемых в книге телефонов приведена востребсванная информация по программаторам-боксам и DATA-кабелям, а именно: принципиальные схемы, порядок работы, различные справочные материалы по конфигурации и назначению выводов системных разъемов телефонов.

Кроме того, в книге приводятся описания основных программных пакетов для работы с сотовыми телефонами основных торговых марок, представленных на российском рынке.

Отдельной главой в книге выделен **материал по универсальным боксам, которые можно изготовить самостоятельно в домашних условиях**.

Ценность предлагаемого издания заключается в его универсальном характере — помимо конкретных моделей **рассматриваются аппаратные платформы, на которых выполнены серии, включающие в себя до десятка моделей телефонов**.

Глава 1. Сотовые телефоны SIEMENS

Модель: «Siemens S35»

Необходимое оборудование

Оборудование, необходимое для программирования большинства сотовых телефонов (и, в частности, «Siemens S35») не отличается особой сложностью:

— персональный компьютер (ПК). Причем, его основные параметры совершенно некритичны: в нем не нужны «навороченная» видеокарта, процессор с высокой тактовой частотой или большой объем оперативной памяти. Для этих целей подойдет почти любой офисный ПК. Единственное необходимое условие для него — наличие COM-порта (RS 232);

— DATA-кабель, который служит для сопряжения системного соединителя сотового телефона и ПК (через COM-порт).

Кроме того, необходимо специальное программное обеспечение (ПО) на ПК, но на этом мы остановимся позднее Внешний вид рабочего места по программированию сотовых телефонов показан на рис. 1.1.

Каждый DATA-кабель должен соответствовать модели телефона. Как правило, маркировка кабеля наносится на корпус одного из его соединителей. Кабель имеет два соединителя, в корпус одного из которых встроена схема преобразователя уровней (сигналов интерфейса RS 232

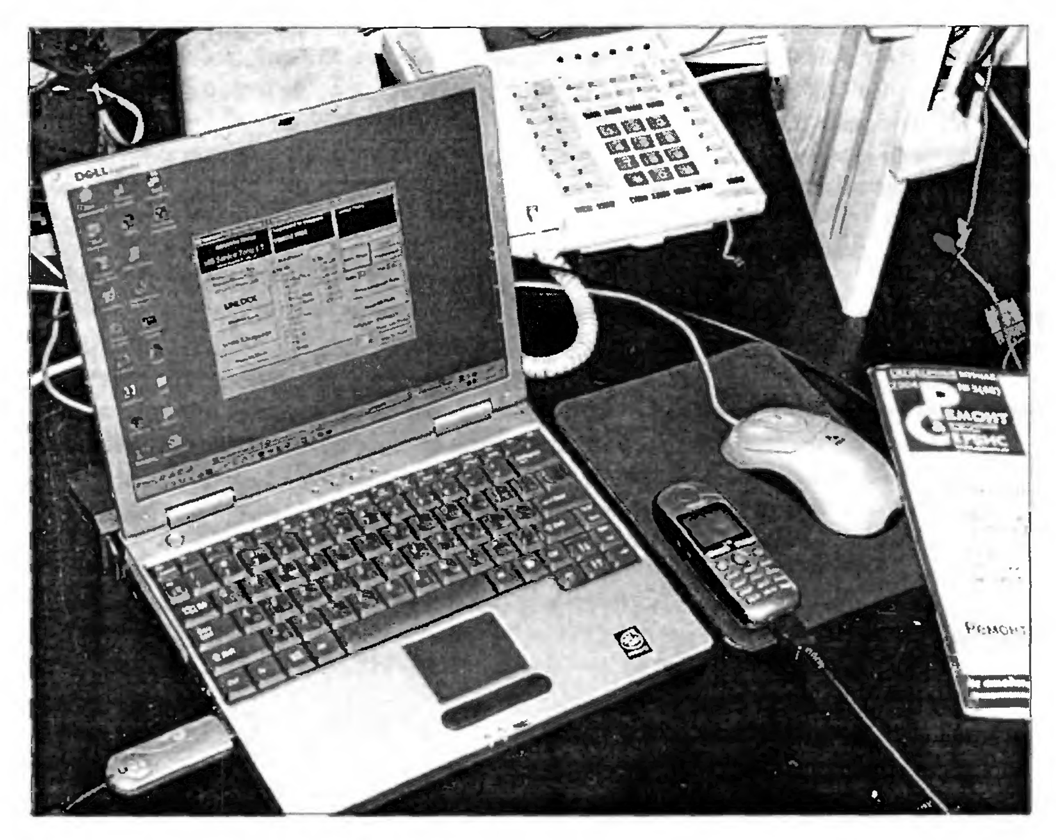


Рис. 1.1

в сигналы с уровнями TTL). В нашем случае преобразователь выполнен на распространенной микросхеме MAX3232. Вариант компоновки схемы приведен на рис 1.2. Принципиальная схема кабеля представлена на рис. 1.3. Он подходит к сотовым телефонам «Siemens C/S 25, C 28, A/C/M/S 35», а также ко всем аппаратам 45 и 50-серии. Следует отметить, что штатные DATA-кабели не имеют линию включения/выключения телефона (AUTO IGNITION), поэтому, при желании, схему на рис. 1.3 можно доработать (вновь установленные элементы выделены рамкой). Эта линия необходима для автоматического включения телефона после «прошивки» стандартным сервисным ПО — Winswup 32. При отсутствии этой линии телефон включают вручную.

Схему преобразователя DATA-кабеля лучше питать от отдельного нестабилизированного источника питания напряжением 8...10 В Его положительный вывод подключают к входу стабилизатора напряжения 78L05 — конт. 7 (RTS) соединителя RS 232, а отрицательный — к конт. 5 (GND).

Кроме DATA-кабеля многие ремонтники в своей практике используют так называемые универсальные переходники («UNI-BOX» — универсальная коробка), в составе которых уже имеется встроенный преобразователь уровней. Переходники «UNI-BOX» подключены к COM-порту ПК, а второй их соединитель меняется в зависимости от типа сотового телефона (его системного соединителя). Это очень удобно, так как отпадает необходимость в приобретении десятков DATA-кабелей — достаточно иметь один универсальный блок.

Следует отметить, что перед выполнением любых операций с ПО телефона необходимо полностью зарядить его аккумуляторную батарею.

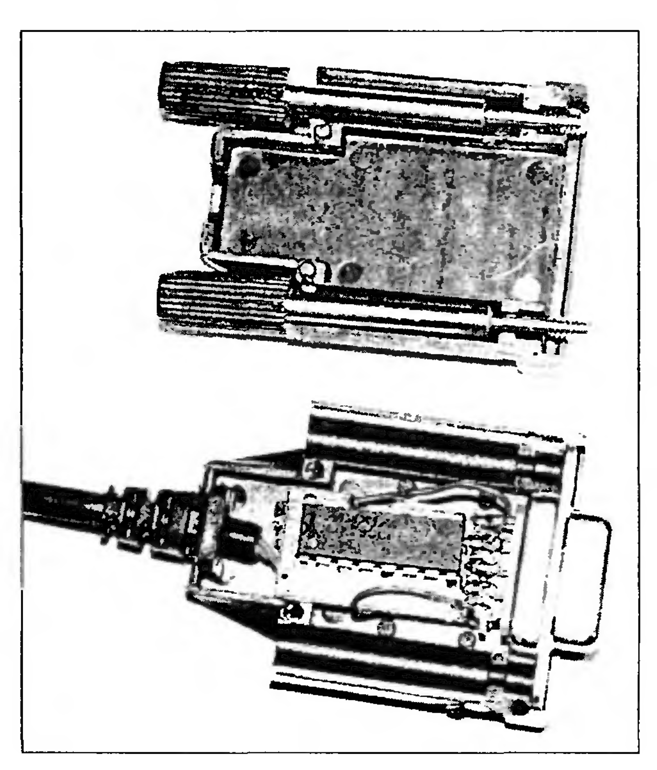


Рис. 1.2

Программирование телефона

Следует отметить, что при использовании указанного оборудования можно выполнять следующие операции по программированию сотовых телефонов «Siemens C/S/M 35»:

- восстановление исходного ПО;
- «русификацию» ПО;
- замена версии ПО на более позднюю;
- регулировку контрастности дисплея (эта операция бывает необходима после замены дисплея);
- сделать резервную копию содержимого памяти аппарата или отдельных его блоков.

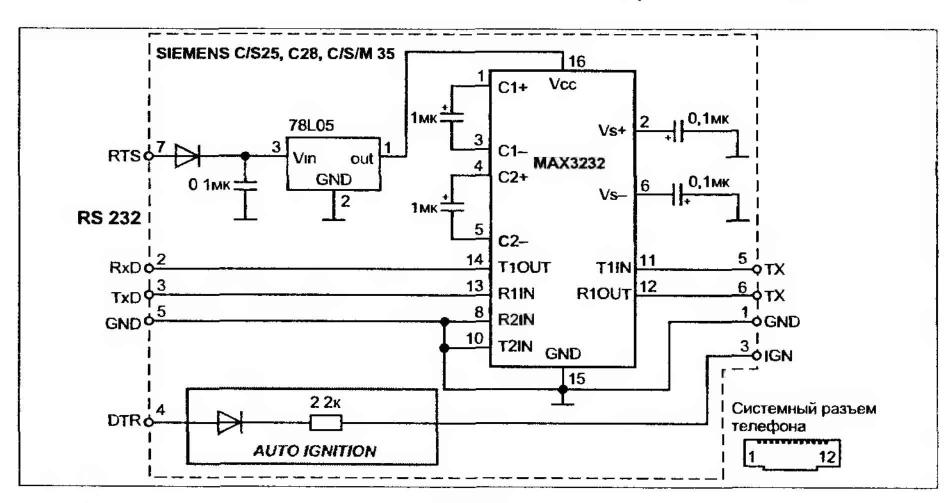


Рис. 1.3

Прежде чем выполнять операции по программированию телефона, необходимо знать текущую версию его ПО. Будем считать, что телефон включается (то есть его аппаратная часть исправна, но есть проблемы с ПО).

Текущую версию ПО телефона можно узнать, набрав на клавиатуре следующую комбинацию: * # 06 *. Эту операцию можно выполнить даже в том случае, если в телефон не установлена SIM-карта. После этого на дисплее отобразится серийный номер телефона (EMEI-номер). Затем нажимают на его левую функциональную кнопку (она показана стрелкой на рис. 1.4) и на дисплее отобразится версия ПО телефона На рисунке видно, что версия ПО — 20.

ПО на телефон можно установить или аналогичное, или более позднюю версию.

Чтобы разобраться, какие языковые пакеты конкретной версии ПО необходимо установить в память телефона, существует программа-подсказка LangInfoGSM (рис. 1.5) Она поддерживает не только аппараты SIEMENS, но и MOTOROLA, NOKIA и ALCATEL.

В меню программы выбирают — «Siemens CSM 35» (1 на рис. 1.5). Зная, что текущая версия ПО нашего телефона 20, в окне 2 выбирают «version 5-20» (2 на рис. 1.5). Затем, меняя положение указателя 3 (Language Pack), в окне 4 находят русский пакет (Russian). Получается, что версия языкового пакета (русский) — 04 (Lang pack 04). Что же касается указателя 5 (T9), то он определяет словарь SMS-сообщений (см. окно 6). Для другой версии ПО, например 24, языковый пакет определяют аналогичным образом. После получения необходимых сведений о соответствии версии ПО языковым пакетам программу LangInfoGSM закрывают.

Рис. 1.4

Затем приступают непосредственно к этапу программирования телефона. Следует отметить, что существует множество программ «прошивки», мы же остановимся на программе, которая называется Winswup 32. Она используется на ПК, работающих под управлением операционной системы Windows.

Загружают на ПК эту программу (рис. 1.6). Первое, что в ней необходимо сделать — сконфигурировать COM-порт ПК, к которому подключен через DATA-кабель сотовый телефон. Для

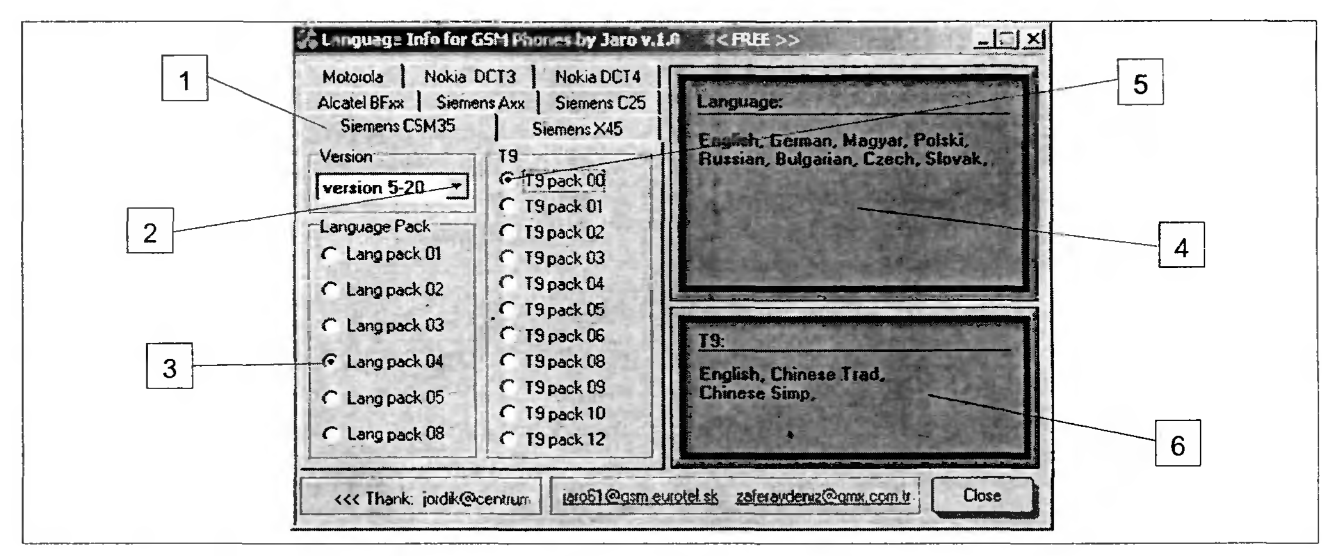


Рис. 1.5

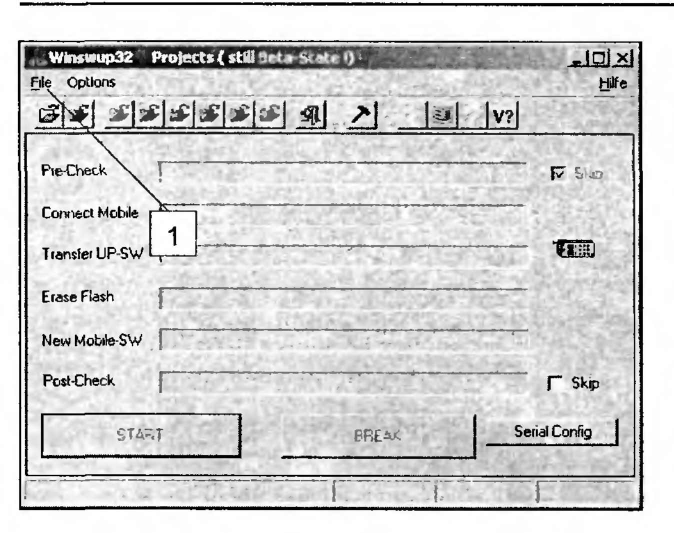


Рис. 1.6

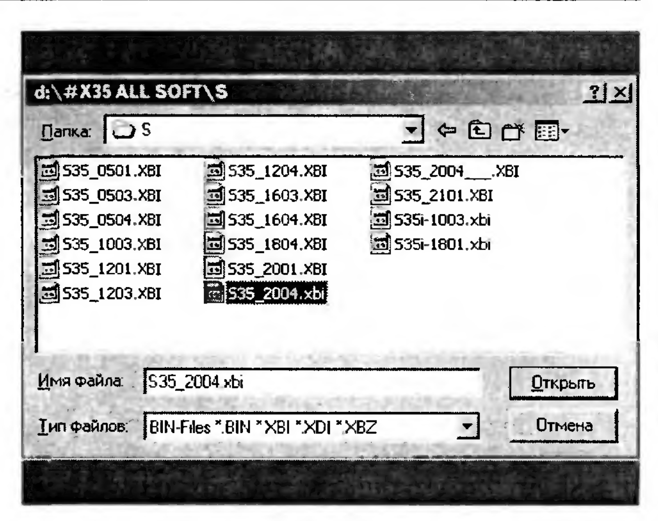


Рис. 1.8

этого нажимают кнопку «Serial Config» (рис. 1.6), после этого появится окно (рис. 1.7). В нем выбирают скорость обмена 115200 (Baud) и номер COM-порта Нажимают «OK» и возвращаются в основное окно (рис 1.6). Нажимают «File» (1 на рис. 1.6), затем «Open» и в появившемся окне указывают путь для выбора файла прошивки (рис. 1.7). Имя файла (S35_2004.xbi) расшифровывается следующим образом:

— тип телефона — S35;
— версия ПО — 20;
— языковый пакет — 04.

Порядок определения двух последних позиций был описан выше.

Выбирают нужный файл и нажимают кнопку «Открыть» (рис. 1.8).

Следует отметить, что существуют два варианта программы Winswup 32 — с прикрепленными файлами прошивки и без них. Если используется программа с прикрепленной прошивкой, то

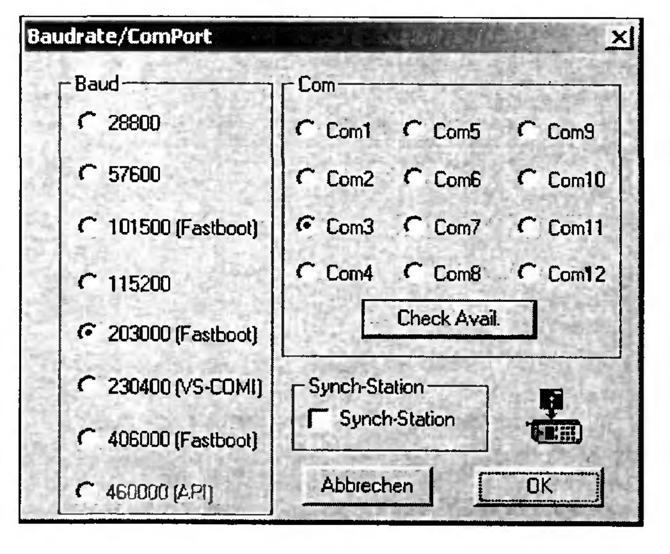


Рис. 1.7

расширение файла имеет вид *.exe. Программа в этом случае имеет объем в несколько мегабайт. В нашем случае используется версия программы без прикрепленных файлов прошивки.

В основном окне программы открывают этот же файл, нажав кнопку 1 (рис. 1.9). В правом окне 2 появляется информация о загруженном файле.

Галочка 3 в строке «Pre-Check» означает, что перед записью ПО не будет выполняться предварительная проверка соединения с телефоном. Галочка 4 в строке «Post-Check» устанавливается, если используется DATA-кабель без доработки AUTO IGNITION (рис. 1.3), чтобы программа не пыталась автоматически включить телефон после прошивки его новым ПО.

Подключают телефон (он должен быть выключен) к ПК через DATA-кабель. Нажимают кнопку 5 «START» и, кратковременно, — кнопку включения телефона (если используется DATA-кабель без доработки). Далее происходит стирание флэш-памяти телефона, при этом в окне программы меняется цвет подложки на оранжевый (рис. 1.10). В момент записи ПО цвет подложки меняется на бирюзовый (рис. 1.11), а в позиции «Erase Flash» справа от шкалы появляется сообщение E401, что означает тип флэш-памяти телефона. Одновременно в позиции «New Mobile-SW» появляется шкала, отражающая процесс записи ПО. Обычно эта процедура занимает около 7 минут. В этот момент на телефоне мигает подсветка клавиатуры и дисплея, причем информация на дисплее не отображается.

Так как в нашем случае был использован не доработанный DATA-кабель, программа прошивки меняет цвет подложки на красный (рис. 1.12) и выдает ошибку. Эта ошибка означает, что отсутствует возможность автоматического включения телефона.

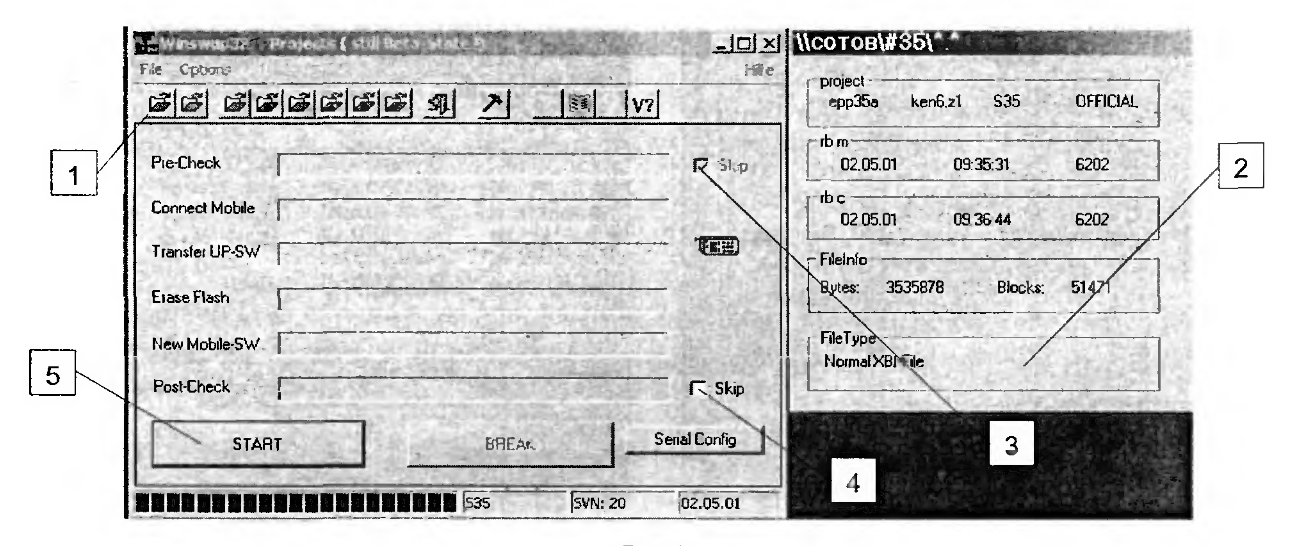


Рис. 1.9

Включают телефон вручную, проверяют версию ПО, а также его работоспособность во всех режимах

Подобную операцию по прошивке ПО выполняют в следующих случаях:

— когда необходима «русификация» телефона,
— при возникновении различных сбоев в работе телефона (некорректная работа ПО),
— для обновления версии ПО (в новых версиях исправляются многие ошибки, выявленные производителем, а также добавляются некоторые дополнительные функции).

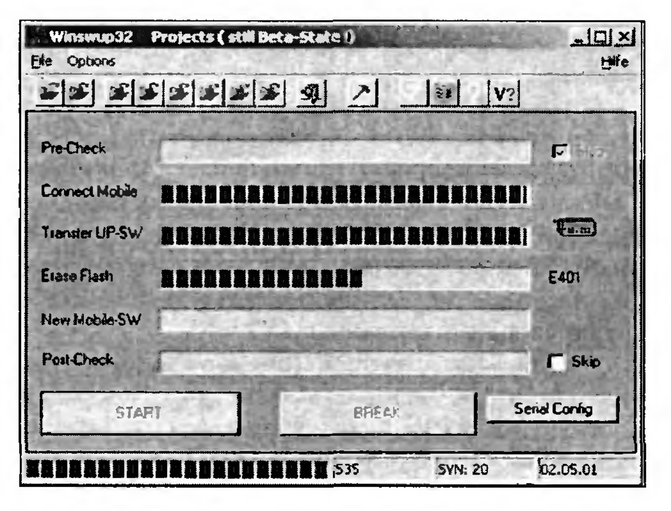


Рис. 1.10

Разблокировка телефона

Прежде чем говорить о порядке разблокировки телефона, остановимся на видах блокировки Всего их две. пользовательская и провайдерская (оператора).

Пользовательская блокировка означает, что неправильно введен код самого телефона (см инструкцию по эксплуатации на телефон, раздел «Безопасность»). Коды SIM-карты (PIN и PUK) к коду телефона (Phone Code) никакого отношения не имеют — они блокируют только SIM-карту. Можно конечно не включать опцию ввода кода,

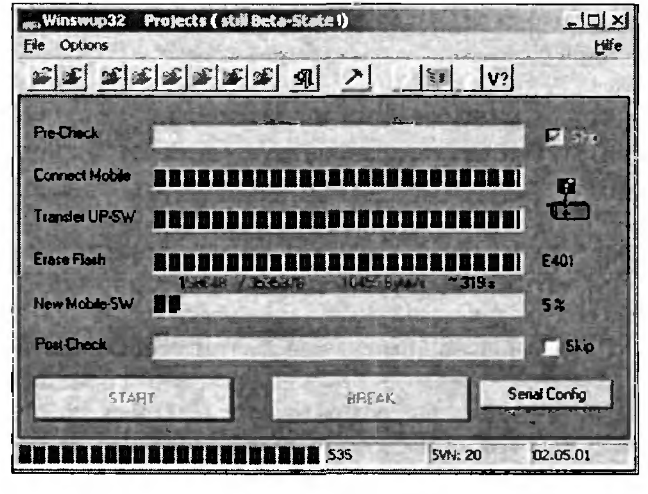


Рис. 1.11

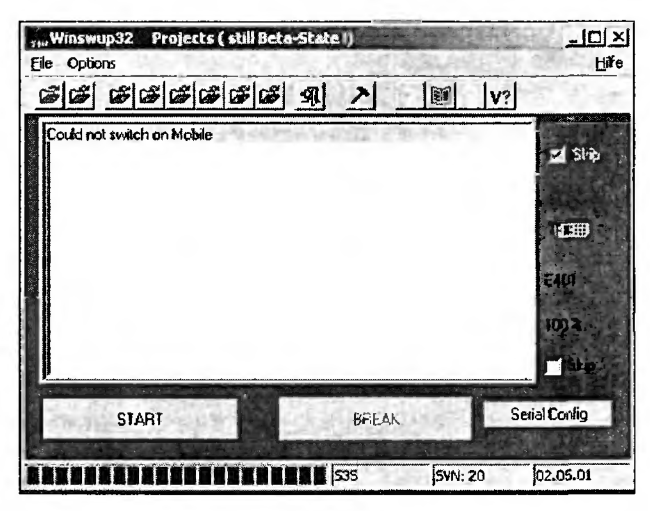


Рис. 1.12

тогда проблема блокировки телефона отпадает сама собой.

Что же касается блокировки провайдера, то многие с ней знакомы, приобретая телефоны, «прошитые» под конкретного оператора — SIM-карты от других операторов в них работать не будут. Код оператора еще называют SP-Lock.

Теперь приступим к методике разблокировки телефонов.

Примечание.

1 Все операции по разблокировке телефона выполняются из его выключенного состояния.

2 Перед тем, как начать программирование телефона, следует убедиться, что аккумуляторная батарея полностью заряжена.

3 Прежде, чем приступать к любым действиям по разблокировке аппарата (и прошивке новой версии ПО), необходимо сохранить резервные копии ПО Более подробно на этом мы остановимся ниже

В качестве примера возьмем программу «Siemens x35 Service Tools» от MARTECH (рис. 1.13). Выбирать тип телефона и его ПО нет необходимости, так как выбрана опция «AutoDetect» (1 на рис. 1.13). На рисунке показана версия этой программы, которая позволяет разблокировать телефоны с ПО до 18 версии. В нашем случае версия ПО — 20, поэтому необходимо найти программу, которая поддерживает соответствующую версию ПО телефона. При разблокировке аппарата, версия ПО которого не поддерживается программой, может привести к печальным последствиям.

Первое, что выполняют — выбирают COM-порт, к которому подключен DATA-кабель с телефоном — каждое нажатие на кнопку 1 будет менять порядковый номер порта.

Входят в сервисный режим телефона, нажав кнопку 3 «Serv. Mode», а на телефоне — кнопку включения питания. В сервисном режиме на дисплее телефона высветится сообщение «Service mode».

Как уже отмечалось выше, выполняют резервные копии ПО телефона (нажав кнопку 1 «Read All Flash» — рис. 1.14) и, желательно, языкового пакета, нажав кнопку 2 «Read Language Area». Эта операция занимает около одного часа.

В сервисном режиме также можно выполнить регулировку контрастности дисплея телефона. Для этого нажимают кнопку 3 «Read From Phone», после этого в окне 6 появится уровень контрастности дисплея, считанный из телефона. При необходимости, меняют эту величину кнопками 4 Нажимают кнопку записи 5 «Write To Phone» и проверяют уровень контрастности на дисплее телефона.

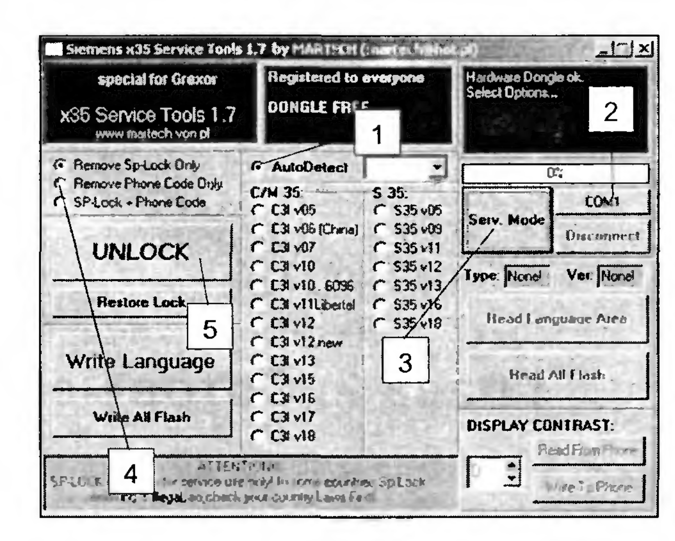


Рис. 1.13

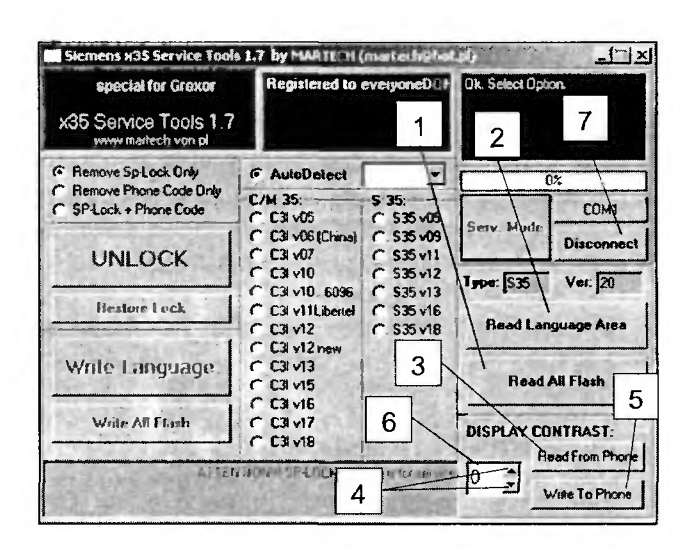


Рис. 1.14

По завершении всех операций в сервисном режиме нажимают кнопку 7 «Disconnect».

Далее переходят к левому окну программы или, собственно, к операции по разблокировке телефона. С помощью кнопок 4 (рис. 1.13) выбирают, что необходимо разблокировать — провайдерскую, пользовательскую блокировки или обе одновременно.

Затем нажимают кнопку 5 «UNLOCK», а на телефоне — кнопку включения питания. Время разблокировки составляет около 5 с.

Отметим также назначение следующих кнопок (рис. 1.13):

«Restore Lock» — восстановить исходную блокировку;

«Write Language» — запись языкового пакета;

«Write All Flash» — записать полную версию ПО.

Две последние операции в основном используются для записи из резервных копий и восстановления ПО телефона.

Глава 2. Сотовые телефоны SIEMENS

Модель: «Siemens C62»

Телефон «Siemens C62» выполнен на платформе Sony Ericsson, со схемотехникой, схожей с моделями T39 и T68 — в них применена аналогичная аппаратная структура, а также используются похожие комплекты микросхем. В связи с этим структура памяти и принцип программирования данной модели схож с программированием аппаратов Sony Ericsson.

Внешний вид телефона SIEMENS показан на рис. 2.1.

Прошивка ПО телефона

Для связи телефона с ПК необходим DATA-кабель, принципиальная схема которого приведена на рис. 2.2. Можно также использовать стандартный кабель от телефонов SIEMENS 55 и 60 серий (кроме ST55/60), предварительно выполнив на нем небольшую доработку — замкнуть между собой попарно конт. 3, 5 и 4, 7 системного соединителя (рис. 2.2). Если же эти перемычки не установлены, с помощью этого кабеля можно выполнять только чтение данных с включенного аппарата, а запись невозможна.

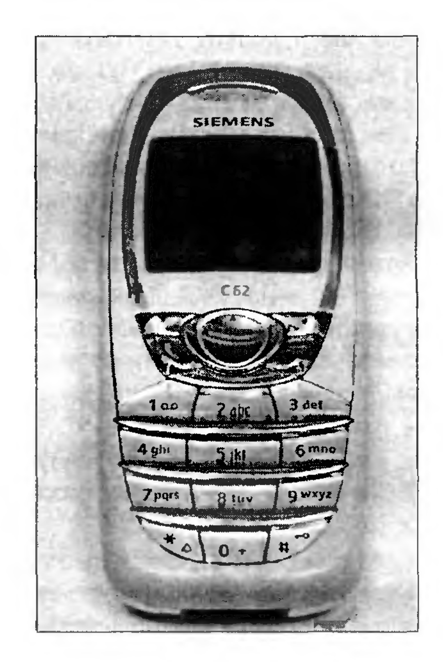


Рис. 2.1

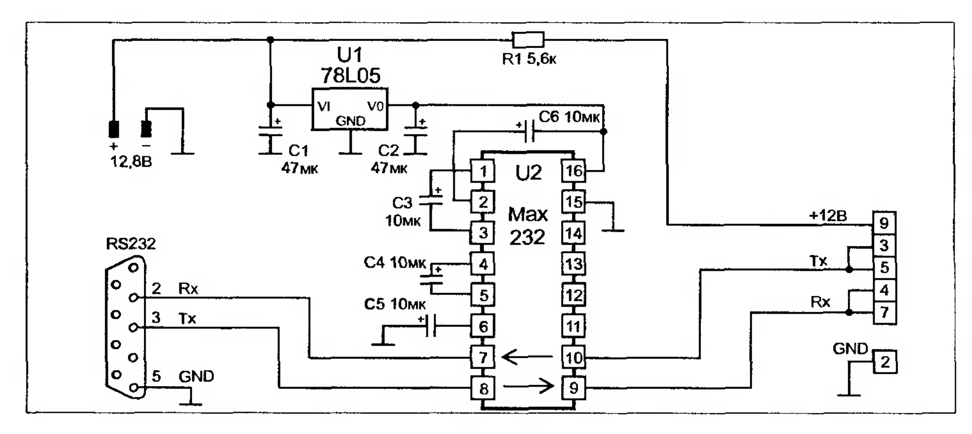


Рис. 2.2

Назначение контактов соединителя телефона приведено в таблице 2.1.

Таблица 2.1

Назначение контактов системного соединителя телефона «Siemens C62»

Номер контакта	Обозначение сигнала	Вход (I)/ выход (O)	Назначение
1	POWER	I	Вход от зарядного устройства
2	GND	–	Общий провод зарядного устройства
3	TX/D+	O	Передаваемые данные с телефона для программирования FLASH-памяти
4	RX/D–	I	Принимаемые данные телефоном для программирования FLASH-памяти
5	DATA/CTS	I/O	Набор сигналов для подключения модема, а также внешних аксессуаров и записи ПО во FLASH-память телефона
6	RTS	I	
7	CLK/DCD	I/O	
8	Audio L	O	Выход звукового сигнала (левый канал)
9	Audio Ref/Vpp	I	Напряжение питания (+12 В) для программирования FLASH-памяти
10	Audio R	O	Выход звукового сигнала (правый канал)
11	GND Micro	–	Общий провод микрофона
12	Micro	I	Вход микрофона

Следует отметить, что во многих источниках принципиальная схема DATA-кабеля имеет ошибку — на входе питания (+12 В) включен последовательно диод, резистор R1 исключен. Для того, чтобы при программировании телефона не возникало ошибок и сбоев, схему кабеля необходимо выполнить, как показано на рис. 2.2, а питающее напряжение должно составлять 12,8 В. Резистор же необходим для ограничения тока при программировании FLASH-памяти.

Для программирования телефона «Siemens C62» необходима программа FLASH PROGRAMMER (внешний вид ее окна показан на рис. 2.3). В свободном доступе распространена ее версия V2.78. Эту программу необходимо установить на ПК, запустив файл FlashProgrammer.exe (1 на рис 2 4). После этого на рабочем столе ПК появится соответствующий значок программы.

Программа позволяет программировать FLASH-память телефона — основную область (MCU-FLASH), языковые пакеты (Language Pack) и так называемую область GDFS (Customization Pack), включающую настроечные таблицы телефона. Данный пакет позволяет программировать только всю область FLASH-память целиком.

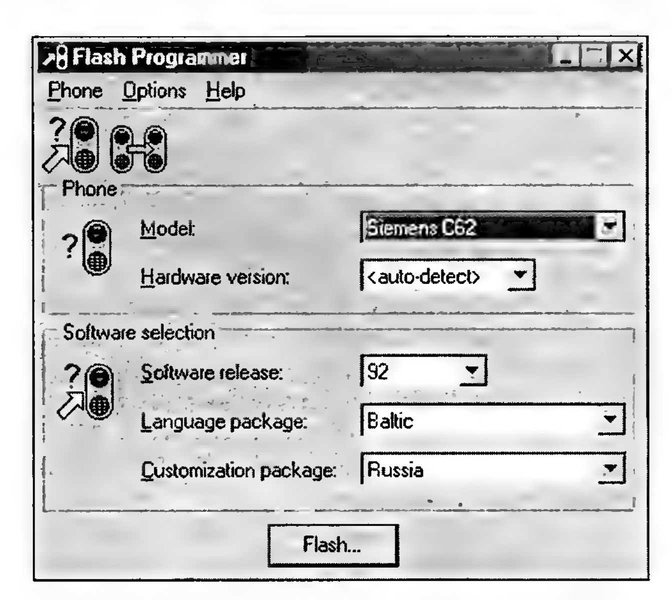


Рис. 2.3

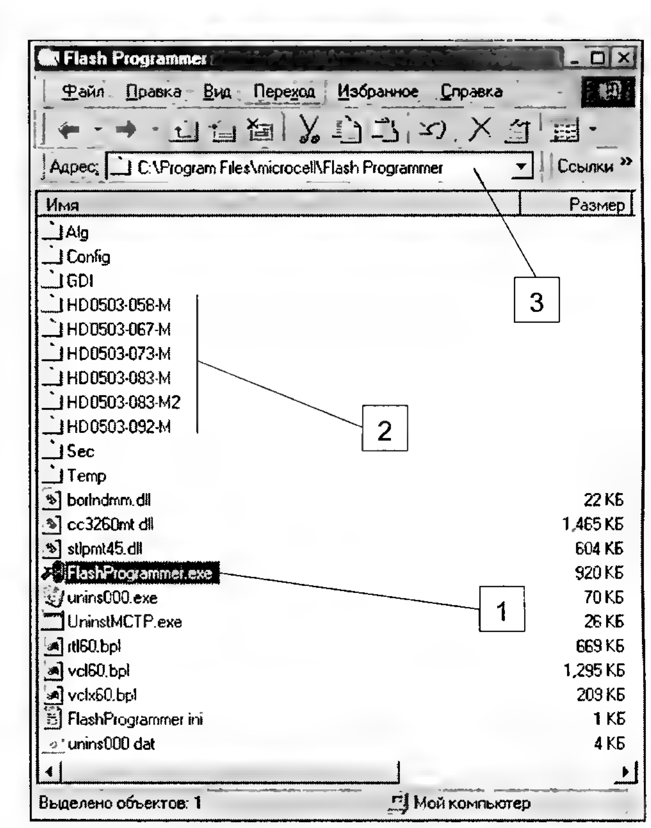


Рис. 2.4

Однако, для того, чтобы программировать по отдельности перечисленные выше составляющие, «поверх» FLASH PROGRAMMER ставится специальный «патч», одно из названий которого может — fffs.exe.

Кроме того, для программирования телефона необходим файл прошивки.

Имя его папки пишется только строчными буквами и имеет вид, например — HD0503-092-M (2 на рис. 2.4). Если буквы в названии будут строчными, программа не найдет файлы прошивки.

Цифры 092 в названии означают номер версии файла прошивки.

Внутри этой папки есть еще три — CUST, FLASH и LANG.

В папке CUST находятся так называемые файлы «кустомизации» (или специальные «настроечные» файлы в табличном виде). «Настроечный» файл для России имеет вид: HD0503-092-M-132.CUS. Там же должен быть файл с таким же названием, но имеющий расширение SSW. Эти два файла дополняют друг друга, и программа без любого из них работать не будет. Проще можно сказать, что папка CUST «отвечает» за содержимое GDFS-области FLASH-памяти телефона.

Папка FLASH содержит файл прошивки MCU-FLASH (см. выше). Он может, например, иметь следующее имя· HD0503-092-001-M.SSW.

В папке LANG находятся файлы языковых пакетов Один из них может иметь следующее имя: HD0503-LNG-092-M-04.SSW. Кстати, для России, кроме 04 (кодировка MEDITERRANEAN), в имени файла могут стоять цифры 90 (ISRAEL) и 91 (BALTIK). Последняя версия имеет русскоязычный словарь T9 для SMS, поэтому он используется наиболее часто.

Программа после инсталляции будет установлена по следующему адресу: C.\Program Files\microsell\Flash Programmer (3 на рис. 2.4).

Для нормальной работы программы папка HD0503-092-M должна находиться в директории Flash Programmer (2 на рис. 2.4).

Чтобы узнать текущую версию ПО телефона, на его клавиатуре набирают следующую комбинацию: *#06# , а затем кнопку Info. После этого на экране отобразится информация, как показано на рис 2.5. Сообщение «SW-Version: 26» означает, что текущая версия ПО соответствует 92-ой версии файла прошивки. Если версия другая, необходимо обратиться к таблице соответствия версий, например, еще одной распространенной версии 20 соответствует прошивка 83.

На рис. 2.5 языковой пакет ПО телефона имеет версию 91 (BALTIK) и словарь SMS — T9 (см. выше).

После определения файла прошивки далее приступают к настройке программы FLASH PROGRAMMER.

Загружают программу и нажимают последовательно кнопки OPTIONS и SETTINGS. В открывшемся окне Settings (рис. 2 6) вначале выбирают опцию C62 (1 на рис 2.6), а затем скорость обмена через COM-порт — 115200 бит/с (2). Потом нажимают кнопку Ports (3) и в окне Configure Ports (4) выбирают номер COM-порта (5).

Нажимают кнопку OK на последнем окне (4), выбирают путь к директории Flash Programmer,

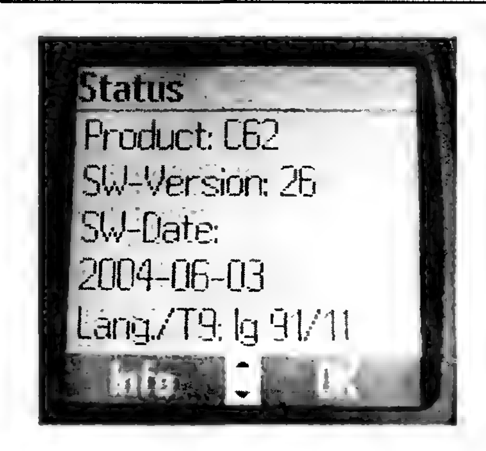


Рис. 2.5

нажав кнопку 6. Справа (рис. 2 7) появится окно 1, выбирают папку Flash Programmer, нажимают кнопку OK и в окне 2 появится аналогичная директория.

После этого закрывают программу и вновь запускают.

В окне программы с помощью ниспадающих меню (рис. 2.8) выбирают тип телефона (C62) — <auto-detect> — версию ПО (в нашем случае 92) — языковый пакет (Baltik) — Russia.

После этого подключают DATA-кабель к выключенному телефону и нажимают кнопку Flash (1 на рис. 2 8). Появится окно (рис. 2.9), сообщение «Please restart the phone» на котором означает, что для начала прошивки необходимо кратковременно нажать кнопку включения телефона.

После этого можно наблюдать процесс (рис. 2.10) прошивки FLASH-памяти телефона. По времени он занимает около 10 минут.

В процессе прошивки могут возникнуть ошибки (например, ERROR BLOCK 74 или ERROR 6), но в большинстве случаев они могут быть вызваны проблемами с DATA-кабелем (сбои питания) или если в процессе настройки программы не выбрана опция Recovery Flash (рис. 2.11).

С помощью программы FLASH PROGRAMMER также можно получить служебную информацию о телефоне Нажав кнопку Show Information (2 на рис. 2.11), появится окно (рис. 2.12), в котором приведены данные о ПО, IMEI-номере, дате изготовления и др. Телефон при этом должен быть включен.

Кроме того, программа позволяет сохранять и удалять пользовательские настройки аппарата. Для этого необходимо нажать, соответственно, кнопки 3 и 4 (рис. 2.11).

Как отмечалось. после установки FLASH PROGRAMMER ставится «патч», который позволяет выбирать файл для программирования телефона по отдельности: MCU-FLASH, языковые пакеты или GDFS. После установки «патча» в окне программы появляется опция Flash File (5 на

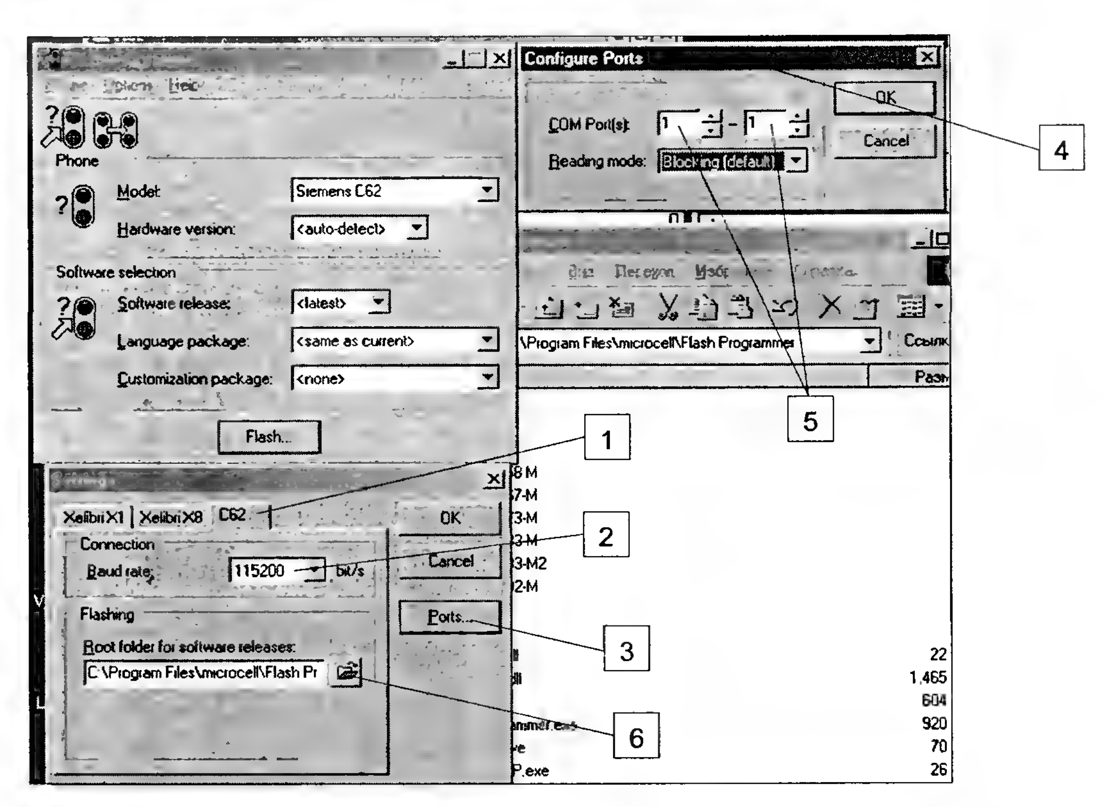


Рис. 2.6

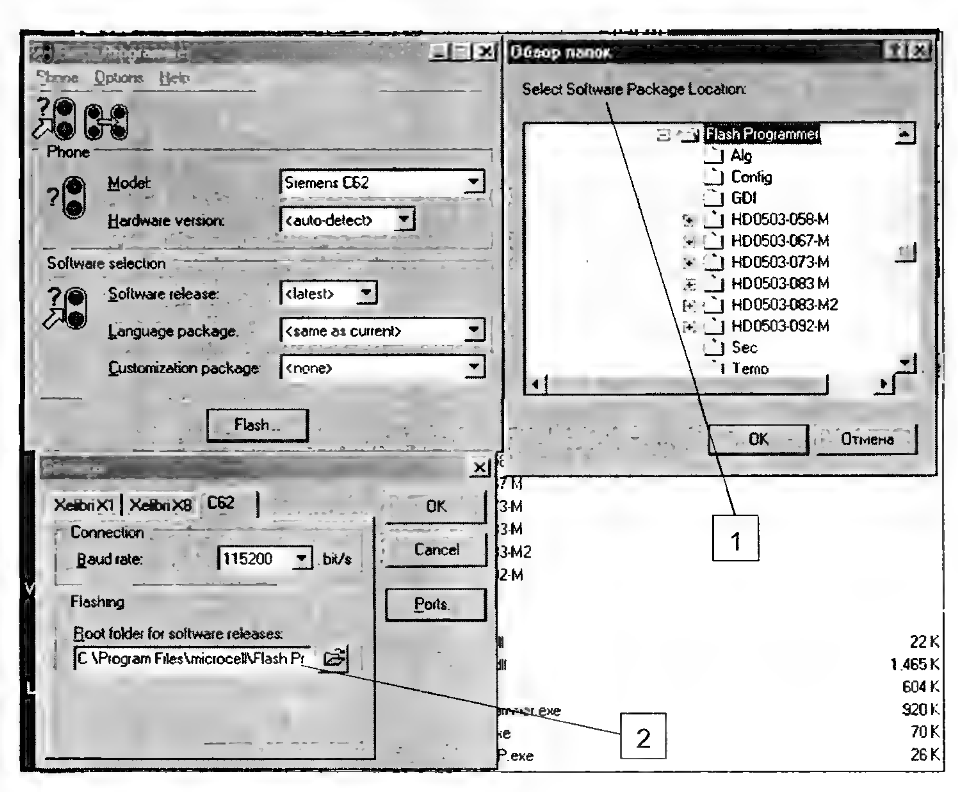


Рис. 2.7

рис. 2.11), при активации которой появляется окно для выбора нужного файла (рис. 2.13), а затем сразу окно начала «прошивки», показанное на рис. 2.9.

Также отметим, что эта программа позволяет прошивать аналогичную или более старшую версию ПО. Хотя, один момент, когда возможна запись и более младшей версии ПО. Для этого переименовывают имена используемых для программирования файлов и папок на более высокую версию. Например, если на телефоне установлена версия ПО 92, а необходимо уста-

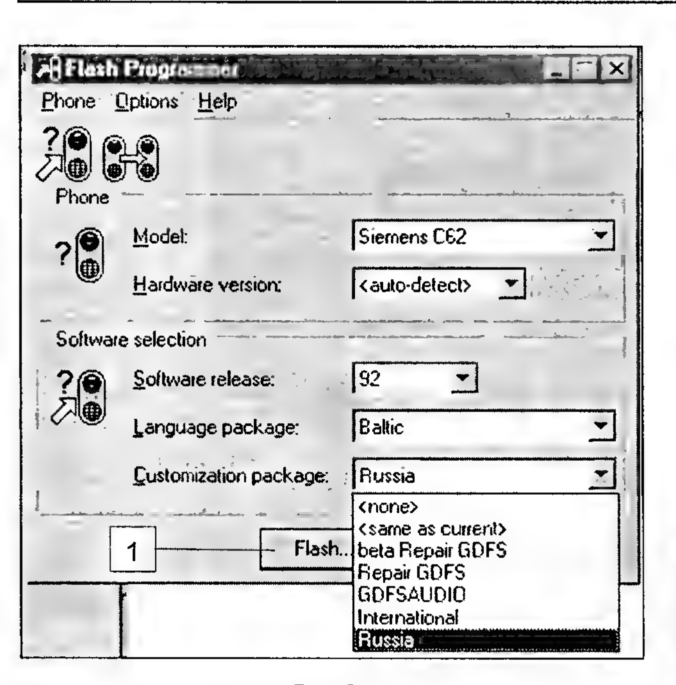


Рис. 2.8

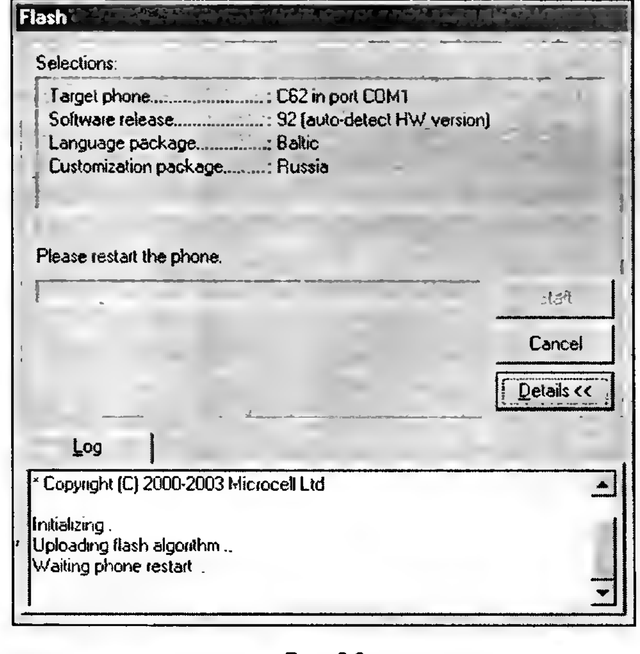


Рис. 2.9

новить 83, во всех именах 4-х файлов (MCU, LANG, GDFS) младшей версии число 83 меняют на 92, а затем программируют телефон.

Разблокировка телефона

Способ 1

Аппарат можно разблокировать, если в GDFS-область FLASH-памяти телефона записать так называемый «ремонтный» GDFS-файл (см. ниже).

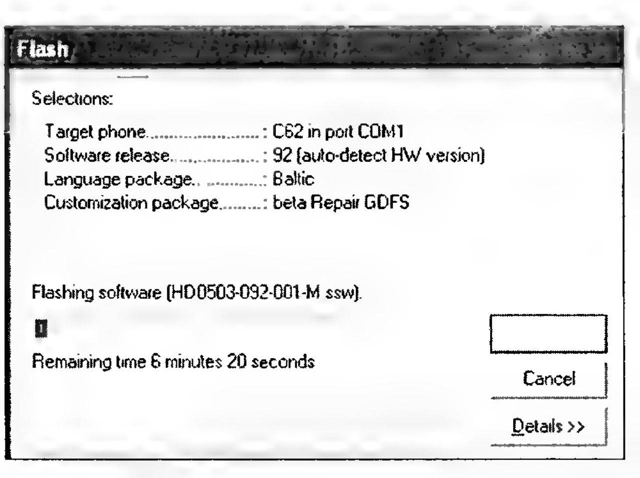


Рис. 2.10

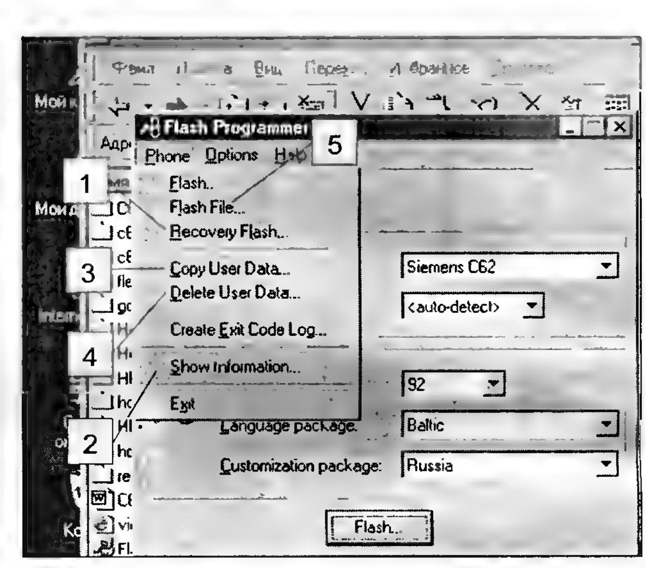


Рис. 2.11

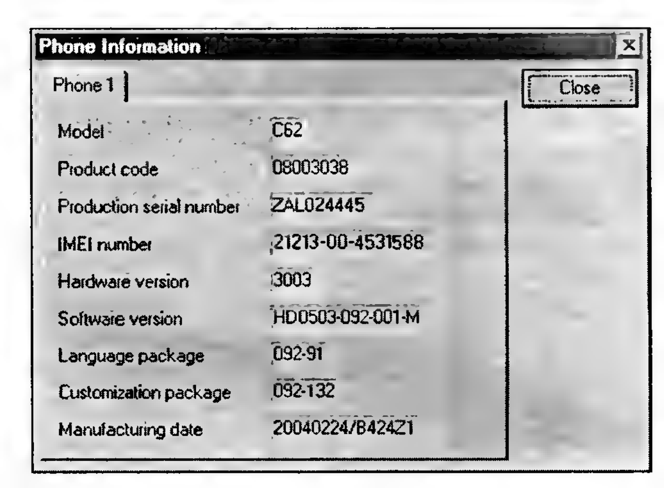


Рис. 2.12

Способ 2

Для разблокировки телефона можно использовать специальную программу C62 logger.exe, доступную в Интернете. Ее окно показано на рис. 2.16.

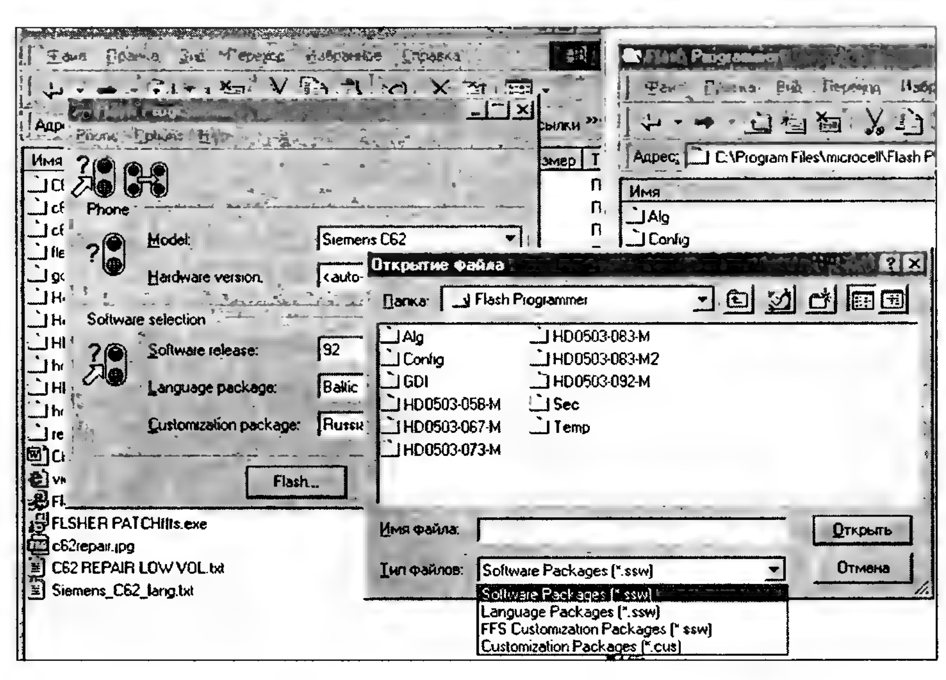


Рис. 2.13

Эта программа определяет коды разблокировки, которые можно ввести с клавиатуры. В окне программы нажимают кнопку Read log (1 на рис. 2.16) и, кратковременно, кнопку включения питания телефона. Если процесс определения кодов разблокировки прошел успешно, окно программы будет иметь вид, показанный на рис. 2.17.

В строке 1 можно увидеть, что пользовательский код телефона — 0000, а в строке 2 отображается сообщение, что сформирован и сохранен файл (IMEI-номер).log. В этом файле размещена необходимая информация для подсчета остальных кодов блокировок телефона, вводимых с клавиатуры. Для прочтения этого файла необходима программа, называемая C62_log_decrypter.exe. Ее окно после загрузки имеет вид, показанный на рис. 2.18. Затем нажимают кнопку Decpypt LOG File. После чего в окне появятся коды разблокировки и блокировки телефона (рис. 2.19). Эта программа поддерживает разблокировку телефонов с версией ПО до 20 включительно. Если же в телефоне используется версия ПО, например, 26, то информация в окне будет отображаться некорректно — в 16-ричном коде (рис. 2.20). Это связано с тем, что производителем в версиях ПО выше 20-й были изменены адреса кодов блокировок в памяти телефона.

Возможные неисправности телефона и способы их устранения

Телефон не включается

В этом случае выполняют полную прошивку FLASH-памяти телефона ПО, как было описано выше. Желательно перед прошивкой включить опцию Recovery Flash (рис. 2.11).

При воспроизведении различных мелодий, «скачанных» из Интернета (файлы с расширением .mid), в телефоне выходит из строя полифоническая динамическая головка. При этом мелодия воспроизводится с малым уровнем громкости через телефонный капсуль, который используется во время разговора

Причина возникновения дефекта заключается в том, что некоторые из «скачанных» файлов имеют установленную программную громкость, равную 128. При их воспроизведении полифоническая звуковая головка (1 на рис. 2.14) телефона перегружается и у нее обрывается обмотка. Головка восстановлению не подлежит, ее необходимо заменить. Чтобы предупредить возникно-

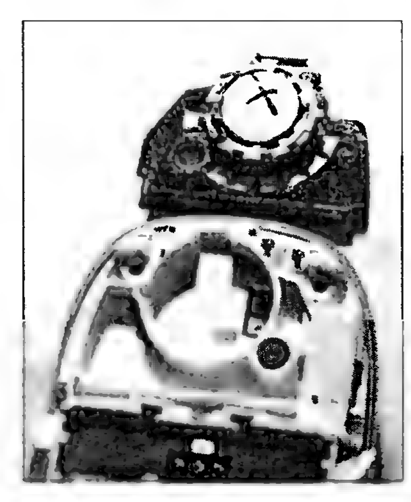


Рис. 2.14

вение подобного дефекта, в меню телефона устанавливают уровень громкости 75% от номинальной.

При воспроизведении полифонических мелодий, их громкость ниже номинала приблизительно на 50% (полифоническая динамическая головка исправна)

Для устранения подобного дефекта необходимо скорректировать GDFS-область памяти. С помощью текстового редактора (программой БЛОКНОТ) открывают GDFS-файл (заканчивающийся на xxxxx132.CUS, например, HD0503-092-M-132.CUS) и вставляют в него «программную» вставку, как показано на рис. 2 15 (она занимает с 2 по 10 строки текста). После этого заново перезаписывают Flach-память телефона.

```
//:title Russia AD
0320 7 0000 04 04 00 05 05 02 00
0321 7 0000 04 02 03 05 05 02 00
0322 7 0000 04 00 03 05 08 02 00
0323 7 0000 01 02 03 04 08 01 00
0324 7 0000 01 02 03 05 05 01 00
0325 4 0000 00 00 00 00
0326 12 0000 01 02 01 04 01 02 00 02 01 03 01 02
0328 7 0000 01 03 03 05 08 02 00
0329 1 0000 03
0033 7 0000 30 39 32 2D 31 33 32
00DE 8 0000 00 01 01 01 01 01 01 01
00DD 6 0000 0C 00 00 00 00 00
00E0 2 0000 01 01
0018 1 0000 01
0175 1 0000 02
00D4 1 0000 06
043D 4 0000 1E 21 00 00
```

Рис. 2.15

Телефон блокируется после некорректной разблокировки программным продуктом от ZULEA, причем, при нажатии комбинации кнопок *#06# его IMEI-номер имеет вид: 099999-91-234567

Если набрать на телефоне комбинацию следующих кнопок. *#0606#, на экране будет отображено, что включены все блокировки («закры-

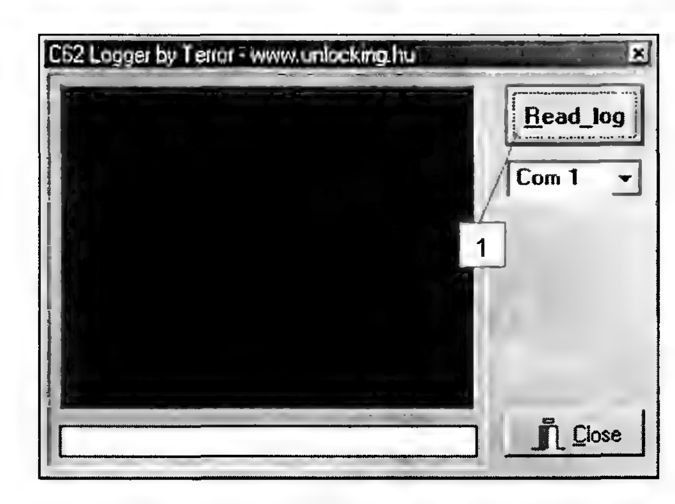


Рис. 2.16

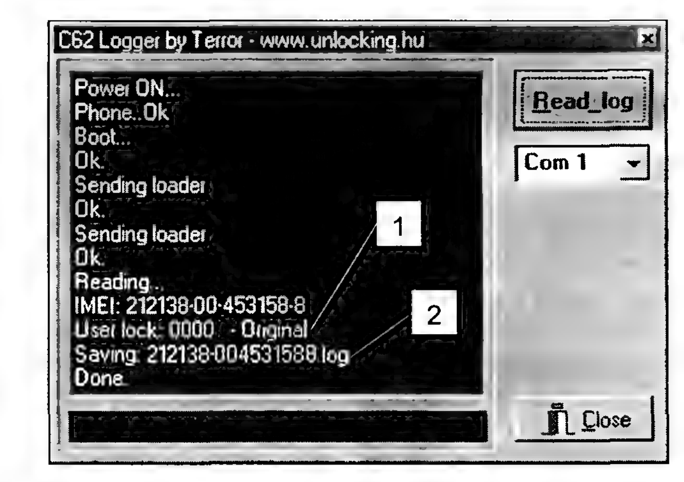


Рис. 2.17

Рис. 2.18

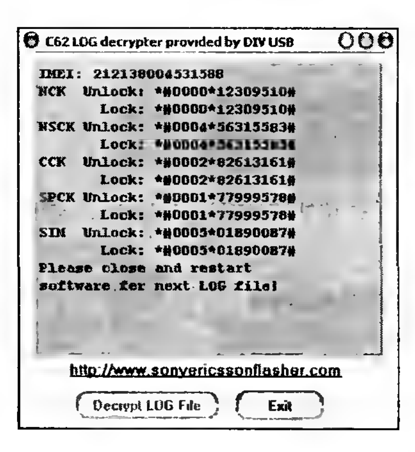


Рис. 2.19

Рис. 2.20

ты» все замки)

Подобный дефект можно устранить, если прошить FLASH-память телефона специальным «ремонтным» GDFS-файлом для 20-ой и 26-ой (83-ей и 92-ой) версий ПО (расширение .CUS). Название файла не приводится, так как он имеет несколько имен (в разных редакциях).

Из «платного» ПО для решения подобной проблемы можно порекомендовать программные продукты от Griffin Team (для C62), например — Direct Unlock C62.

Также «дефектный» IMEI-номер появляется (одновременно блокируется телефон) после замены одной из микросхем — процессора или FLASH-памяти. Чтобы этого не происходило, указанные микросхемы необходимо менять парами (в крайнем случае, микросхема FLASH-памяти должна быть «чистой»).

Глава 3. Сотовые телефоны SIEMENS

Телефоны SIEMENS 45, 50, 55 и 60-ой серий

Сотовые телефоны SIEMENS серий 45, 50, 55 и 60-ой являются одними из самых массовых в нашей стране. Не смотря на их «немецкое» качество, эти аппараты являются частыми «гостями» сервисных организаций. По этим моделям у ремонтников всегда было много вопросов, а больше всего — по восстановлению программного обеспечение. Прежде чем подробно рассматривать эту тему, остановимся на некоторых моментах, которые необходимо учитывать при программировании этих телефонов.

Управляющие программы (УП) для прошивки аппаратов «Siemens C45/S45/ME45/SL45/A50/A52», а также аппаратов 55-й и 60-й серий во многом схожи. Исключение составляют телефоны «Siemens ST55/ST60/C62» выполнены на другой платформе — для них необходимы другие УП. Этот момент необходимо учесть. Материалы об особенностях программирования телефона «Siemens C62» были опубликованы в главе 3.

Также отметим следующее: во всех моделях телефонов SIEMENS 45-й серии и в модели A50 применяется процессор производства INFINEON марки PMB 6850, а в модели «Siemens A52», всей 55-й и 60-й серий — процессор типа PMB 7850. Вследствие этого программирование моделей с разными процессорами имеет отличие (см. описание программы SST).

Для программирования телефонов с ПК необходим DATA-кабель. Принципиальная схема кабеля для моделей 45-й серии и «Siemens A50» приведена на рис. 3.1. Эта схема является универсальной для всей серии телефонов начиная с 25-ой и заканчивая 50-ой серией. Для моделей 55-ой и 60-ой серий схема кабеля приведена на рис. 3.2.

На примере модели «Siemens C55» рассмотрим наиболее часто используемые программные продукты для этого и других телефонов (перечисленных выше), а также остановимся на особенностях их программирования.

Прошивка ПО, программная инициализация

Если аппарат включается, набирают код ***#06#**, а затем левую кнопку (info) — узнают IMEI-номер, версию ПО телефона, тип языкового пакета и др. Исходя из этой информации выбирают соответствующие файлы для прошивки те-

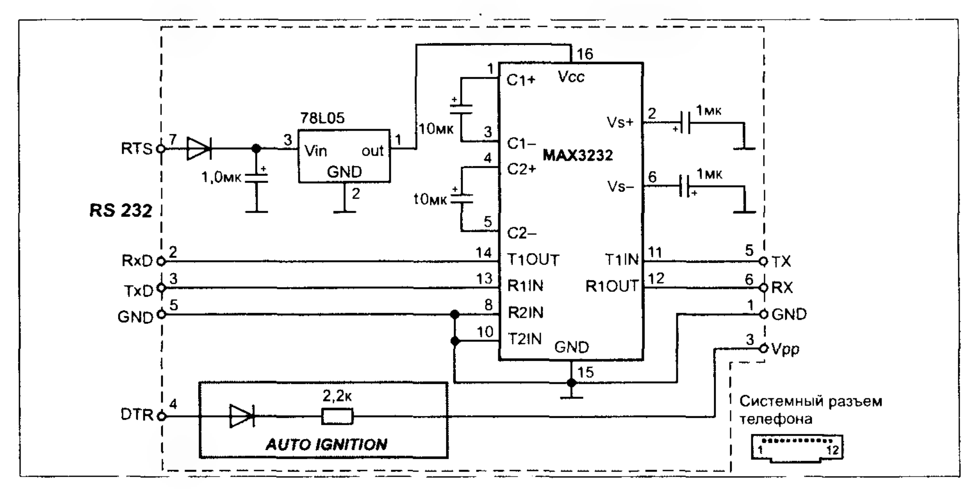


Рис. 3.1

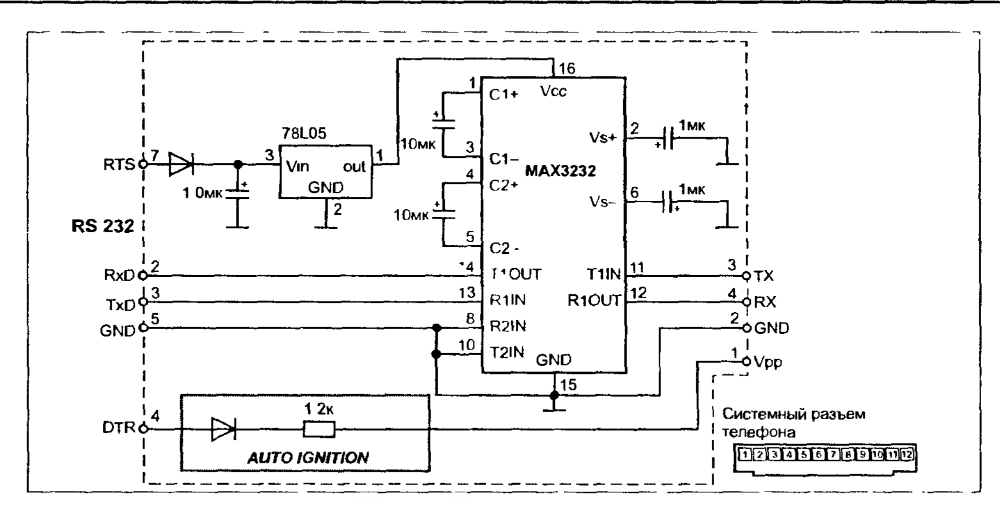


Рис. 3.2

лефона. Перечислим наиболее частые операции, выполняемые с ПО телефона:

— прошивка аналогичной версии ПО или ее новой версии (так называемое «повышение» версии),
— замена (обновление) языкового пакета.

Эти операции, например, можно выполнить с помощью сервисной программы **Winswup 32**. Порядок работы с этой программой для телефона «Siemens S35»описан в главе 1. Загрузочный файл программы для телефона С55 имеет вид. **C55249111.exe** (тип телефона С55, 24-я версия ПО, 91-й языковой пакет, 11-я группа).

Существует программа **C55 UpdateTool,** позволяющая программировать включенный телефон. Основным отличием данной программы от Winswup является то, что в программный пакет включена так называемая область контента, программируемая на встроенную карту ММС и файл загрузки, который, как правило, имеет вид: **C55189111 UpdateTool.exe**. Окно программы показано на рис. 3.3.

Остановимся подробнее на программе Winswup 32.

Внешний вид ее окна после загрузки программы показан на рис 3 4.

После загрузки программы нажимают кнопку «ОК» (1 на рис. 3.4). После этого появляется окно (рис. 3.5), состоящее из двух частей Правая часть (1 на рис. 3.5) выполняет справочную функцию и содержит информацию о типе телефона, версии ПО, языковом пакете и др. Левая часть — панель управления Если на ней нажать кнопку «Serial Config» (2 на рис. 3 5), появится окно настройки портов ПК (рис 3 6).

Приведем пример — допустим, вместо 18-ой версии ПО, 90-го языкового пакета, 11-ой группы необходимо прошить 24-ю версию, 91-й пакет, 11-ю группу. Файл обновленной прошивки будет иметь вид **C55_249111.exe**.

Отметим, что в обоих случаях используется русскоязычный языковый пакет.

В качестве примера файла прошивки **C55_18xxxx.exe** (хххх — цифровое обозначение

Рис. 3.3

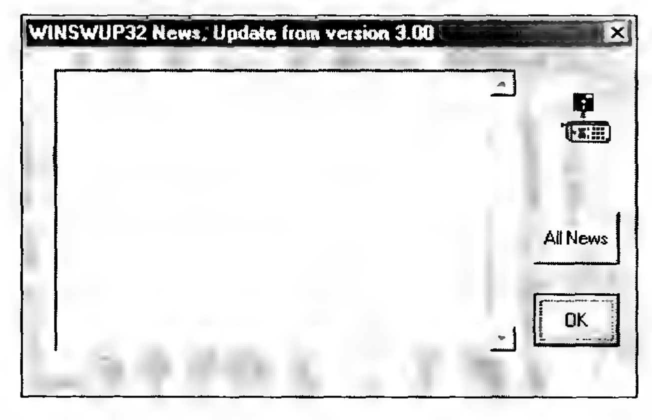


Рис. 3.4

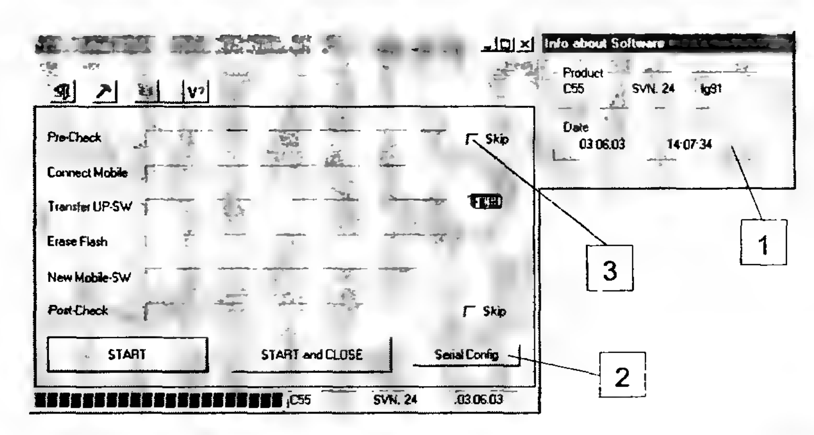


Рис 3.5

языкового пакета) в таблице 3 1 приведено соответствие обозначений некоторых языковых пакетов их содержимому.

Из таблицы видно, что для России предпочтителен языковый пакет **9111** — он имеет русскоязычные пользовательский интерфейс и словарь SMS (T9).

В качестве дополнения хочется рассказать о полезной программе, позволяющей быстро переводить цифры в содержащиеся в пакете языки. Основное окно программы **All New Siemens Lang Info by Mroa v.1.0** показано на рис 3 7. Вам стоит только выбрать модель телефона и последние 4 цифры прошивки — программа сама декодирует и покажет в правых окнах список основных языков меню и языков T9 Этой программой поддерживаются модели от C45 до CX65, любые версии ПО.

Перед началом процесса прошивки телефона необходимо поставить «галочку» в окне 3 (рис 3 5), включающую предварительную проверку включения телефона. После появления окна предупреждения нажимают кнопку «OK».

Примечание. *В некоторых случаях не происходит автоматического включения телефона (программа сообщит об этом) даже если в DATA-кабеле предусмотрена линия AUTO IGNITION (см рис 3 1 и 3 2) Для выхода из создавшегося положения кратковременно нажимают кнопку включения телефона*

Затем нажимают кнопку «START» и контролируют процесс программирования телефона

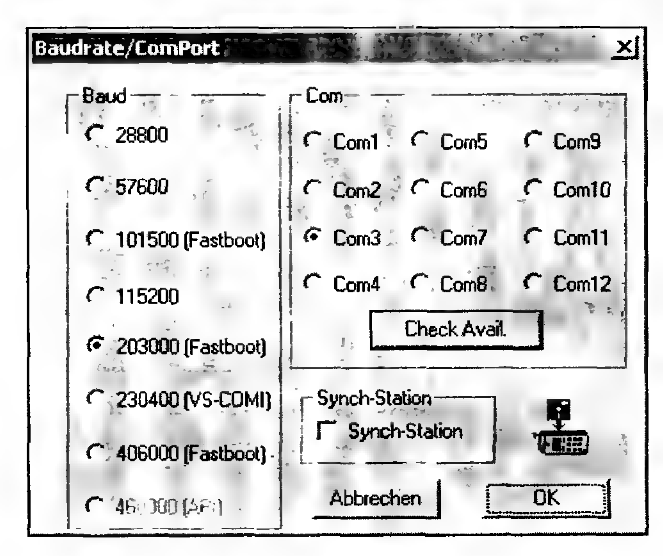


Рис. 3.6

В ходе его выполнения окно программы меняет цвет в зависимости от выполняемой операции Например, при стирании Flash-памяти телефона (Erase Flash), цвет окна — оранжевый (рис 3.8)

В нашем случае обновленная версия ПО — C55_249111 (см. выше) Она имеет объем 4,612 Мбайт При скорости обмена между ПК (COM-порт) и телефоном 115200 Бод время программирования последнего должно составлять около 7 минут

По окончании программирования телефона окно программы будет иметь вид, показанный на рис 3.9

Таблица 3.1

Обозначение языкового пакета	Объем, Мбайт	Языки пользовательского интерфейса	Словарь SMS (T9)
0101	5,08	Английский, немецкий, датский, французский турецкий, итальянский, арабский	Английский, немецкий, французский, итальянский арабский
9010	5,05	Английский, немецкий, французский, русский, итальянский	Английский французский
0109	5,07	Английский, немецкий, французский, турецкий, датский итальянский, арабский	Английский, французский, арабский
9111	5,06	Английский, латвийский, литовский русский, польский, эстонский	Английский, русский, польский

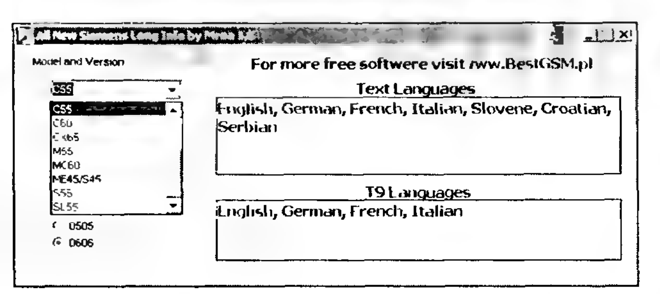


Рис. 3.7

После этого включают аппарат и проверяют версию ПО (в нашем случае, 24-я версия, языковой пакет 9111) Если телефон после пошивки ПО не включается или не выполняет некоторые функции, заново прошивают ранее считанное ПО (так называемую резервную копию его Flash-памяти). Кстати, резервную копию ПО телефона считывают (и сохраняют) во всех случаях перед проведением программного ремонта аппарата.

Если это не дает положительного эффекта, проверяют файлы прошивок, соответствие IMEI-номера в OTP-области и EEPROM и др. В худшем случае принимают решение о проведении аппаратного ремонта телефона.

Перед тем, как приступить к рассмотрению темы по программному сбросу и разблокировке телефонов, рассмотрим распределение их Flash-памяти.

Вся Flash-память телефона делится на следующие области:

- Boot Core (область загрузчика);
- Main Flash (основная память);
- One Touch Programming (OTP или область памяти, однократно программированная производителем),
- Lang (языки);
- область EEPROM (ЭСППЗУ);
- область CONTENT (MMC или FLEX).

Назначение и описание большинства из названных областей Flach-памяти приводится в главах 1, 2 и 5. Остановимся подробнее на области CONTENT.

В этой области помещены картинки, мелодии, JAVA-приложения, звонки, SMS-сообщения, адресная книга и др Из всех телефонов SIEMENS 45-й серии выделяется модель SL45 В ней под область CONTENT выделена съемная карта памяти MMC. В моделях ME45, а также телефонах 50-й и 60-й серий подобная карта уже не предусмотрена, аналогичные функции выполняет соответствующая область общей Flash-памяти.

Отметим, что при прошивке ПО этих телефонов, содержимое области CONTENT не меняется.

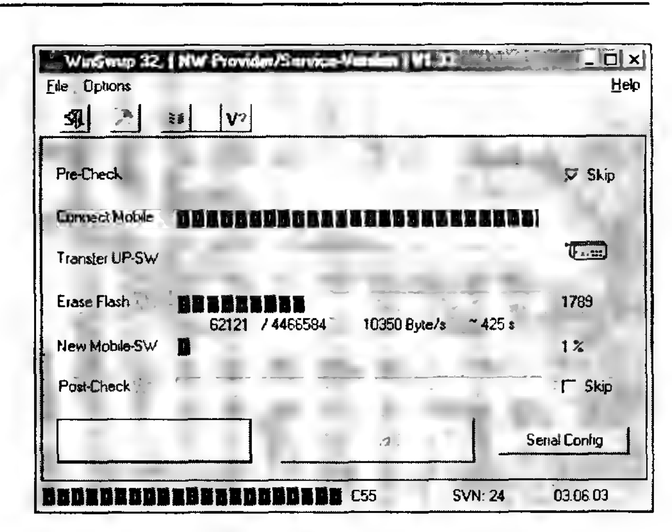


Рис. 3.8

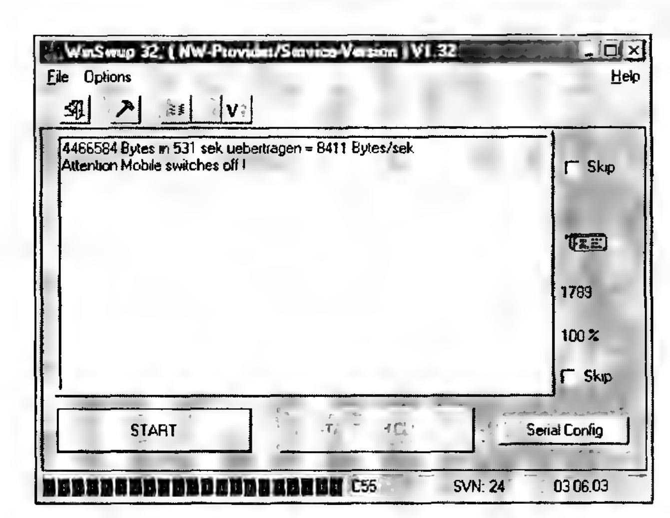


Рис. 3.9

Содержимое CONTENT может меняться пользователем (добавляться или удаляться SMS-сообщения, мелодии и др.). Кроме того, для этих целей существует специальные программы, например, **Siemens Data Suite** и **Data Exchange Software** Они работают с областью CONTENT, не изменяя общее ПО телефона.

Существуют программы инициализации области CONTENT, которые вначале форматируют ее, а затем копируют исходные файлы. Окно одной из этих программ — **Flash File System Initialisation,** показано на рис. 3.10. Для запуска процесса инициализации CONTENT нажимают кнопку 1 «START» Чтобы просмотреть список файлов, которые будут записаны в эту область памяти телефона, нажимают кнопку 2 «Show Initialization Content» После этого появится окно, которое показано на рис 3.11

Разблокировка

Виды блокировок телефонов рассматриваются главах 1 и 5. Для разблокировки указанных выше моделей аппаратов существует целый ряд программ. Остановимся подробнее на наиболее распространенных.

Программа SIEMENS SERVICE TOOLBOX

Программа SIEMENS SERVICE TOOLBOX (или SST) имеет много версий. Рассмотрим одну из них — SST Professional Edition 5.31 Ее особенностью является наличие дополнительных по сравнению с предыдущими версиями функциональных возможностей Эта программа поддерживает наиболее полный список моделей телефонов SIEMENS. Основное окно этой программы показано на рис 3.12. Оно состоит из двух частей EGOLD и SGOLD, каждая из которых «привязана» к своему списку моделей. На самом деле, аббревиатуры EGOLD и SGOLD соответствуют различным сериям процессоров, которые используются в телефонах. Например, EGOLD соответствует сериям процессоров PMB 6850 и PMB 7850.

Порядок работы с этой программой следующий.

Подключают выключенный телефон к ПК через DATA-кабель. Запускают программу SST и выбирают окно в соответствии со списком моделей телефона (в нашем случае модель C55 находится в окне EGOLD), в нем выбирают телефон C55, номер порта ПК (COM1) и скорость обмена (115200 бод).

Для чтения информации о IMEI-номере и серийном номере Flash-памяти вначале выбирают «закладку» MAIN (1 на рис. 3.12) и нажимают кнопку 2 «Read Info». Должно начаться чтение данных из телефона (в DATA-кабеле есть линия AUTOIGNITION, см. рис. 3.1 и 3.2) Если этого не произошло, кратковременно нажимают кнопку включения питания телефона.

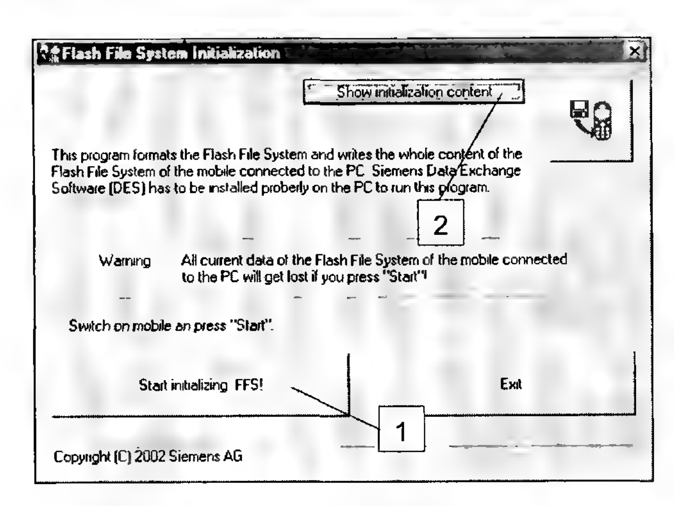


Рис. 3.10

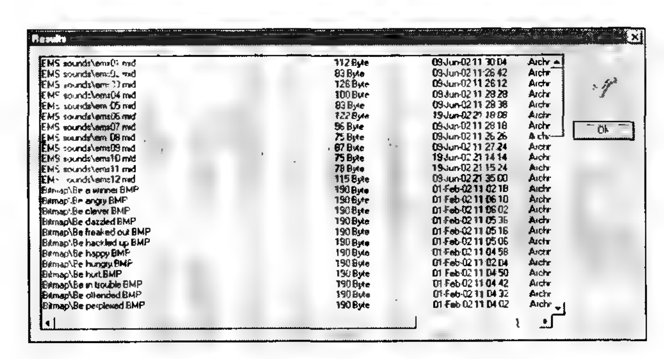


Рис. 3.11

После чтения данных в окнах 3 и 4 отобразятся IMEI-номер и серийный ID номер микросхемы Flash-памяти.

Для выполнения резервной копии MAIN считывают файл прошивки телефона, нажав кнопку 8 «Read Flash» (рис. 3.11). Для открытия файла нажимают кнопку 7 «Open Flash», а для его записи — кнопку 9 «Write Flash».

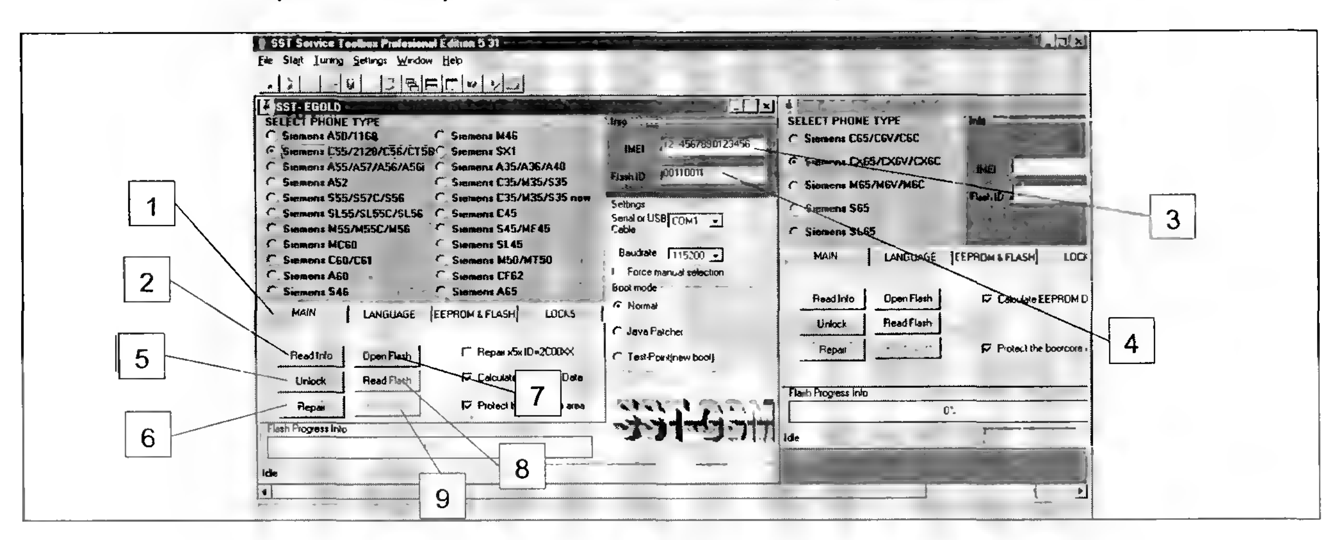


Рис. 3.12

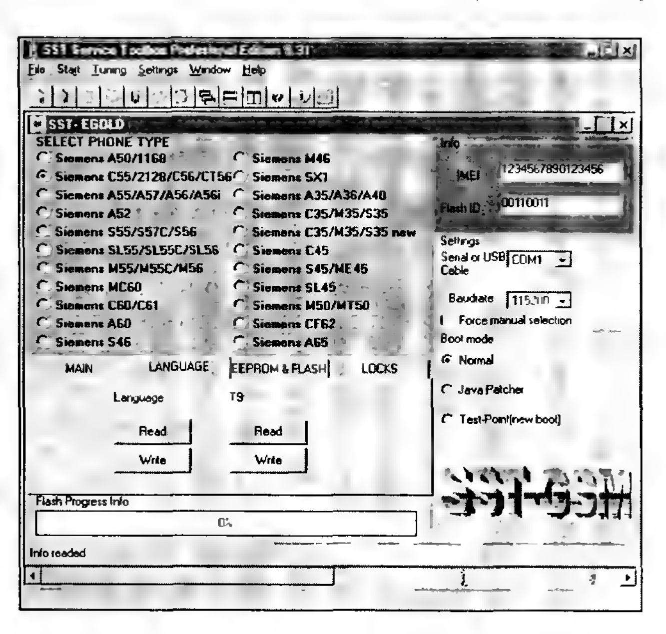


Рис. 3.13

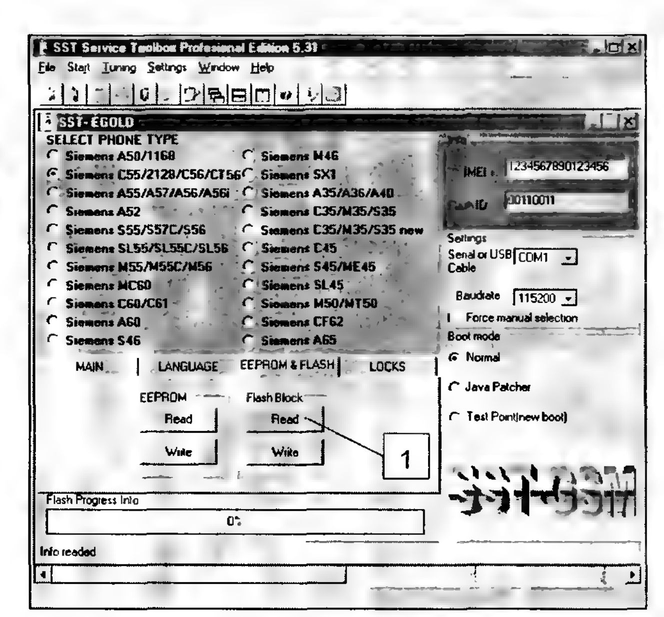


Рис. 3.14

В закладке MAIN, нажав кнопку 5 «Unlock», можно выпонить разблокировку телефона.

Для приведения в соответствие серийных номеров аппарата IMEI (первый находится в области EEPROM, второй — в OTP нажимают кнопку 6 «Repair». Эту операцию чаще всего выполняют, когда аппарат не включается или при нажатии на кнопку включения из динамической головки слышен звук низкого тона Также операцию REPAIR выполняют после перезаписи данных из EEPROM другого телефона или полной перезаписи FLASH. В этом случае серийный номер IMEI считывается из OTP-области телефона и записывается в область EEPROM.

Открывают закладку LANGUAGE (рис. 3.13) — в ней можно отдельно прочитать/записать языковый пакет и словарь T9. Аналогичные операции можно выполнить, выбрав закладку EEPROM&FLASH (рис. 3.14), но с одним отличием — при нажатии кнопки 1 «Read» раздела Flash Block можно выбрать границы чтения адресов Flash-памяти. Аналогично поступают при записи данных. В момент чтения/записи данных во всех перечисленных закладках, появляется прогрессирующая шкала выполнения выбранной операции (см. 1 на рис. 3.15 при выполнении операции чтения области EEPROM).

Отметим, что после завершения операции считывания выбранной области Flash-памяти программа предложит сохранить сформированный файл в бинарном формате.

Закладка LOCKS (рис 3.16) позволяет заблокировать телефон на определенного оператора (например, для отечественного оператора МТС код блокировки 25001). Выбрав код оператора, в этом же окне нажимают кнопку «Lock». После проведения подобной операции, никакие SIM-карты, кроме карт выбранного оператора, в данном телефоне работать не будут.

Перечисленные выше операции по доступу к Flash-памяти (чтению/записи) могут и не выполняться, так как фирма-производитель на многих типах аппаратов предусмотрела защиту. Суть ее в следующем: при внешнем подключении ПК к телефону блокируется доступ к области загрузчика Flash-памяти телефона. Например, в процессорах серии PMB 7850 есть вывод (его буквенно-цифровое обозначение T9), на который принудительно подается лог. «1», запрещающий чтение программы загрузчика Flash-памяти. Это ограничение справедливо только на этапе запуска файла загрузки (из области памяти Boot Core). Если же в начальный момент загрузки на указан-

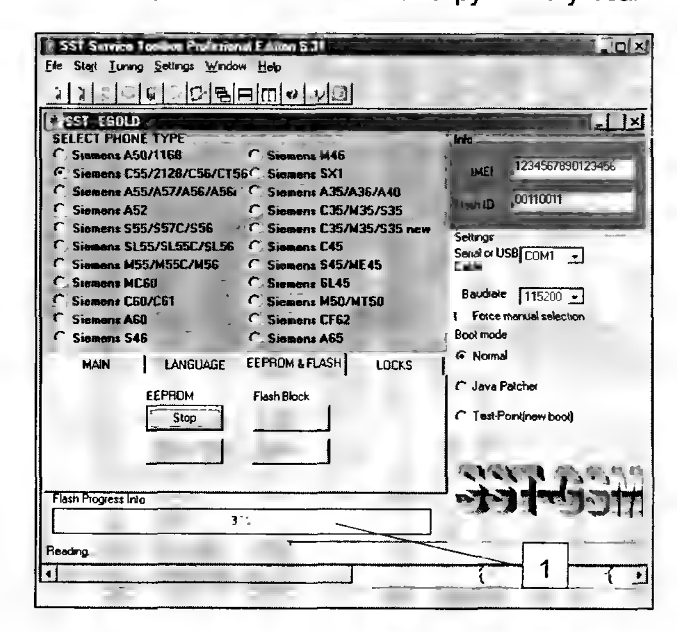


Рис. 3.15

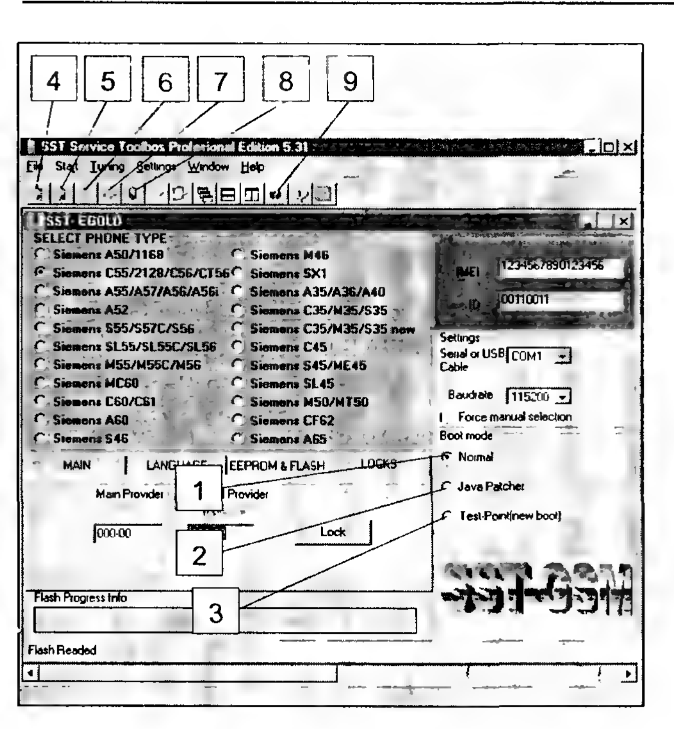


Рис. 3.16

ный вывод процессора кратковременно подать лог. «0», а затем восстановить лог. «1», то программа-загрузчик запустится, и далее все операции между ПК и телефоном будут выполняться без всяких ограничений.

Изменение логического уровня на указанном выводе процессора не обязательно должно быть кратковременным — в большинстве случаев достаточно постоянно отключить вывод Т9 от схемы. Все зависит от конкретного типа аппарата и его ПО (в том числе и версии). Многие ремонтники отключают указанный вывод процессора следующим образом. С помощью паяльной станции выпаивают микросхему процессора с платы телефона. Затем аккуратно (например, с помощью острого жала паяльника) удаляют припой с вывода Т9 как на микросхеме, так и на плате. В заключение, впаивают процессор на плату. В результате вывод Т9 не будет иметь контакта с платой, что соответствует состоянию лог. «0» на нем.

Необходимо отметить, что телефоны, в которых ПО не «опрашивает» логический уровень сигнала на указанном выводе процессора или имеют ошибку в защите (т.н. Bootcore Bug), работают с ПК без каких либо ограничений. Это касается, например, аппаратов М55 (версии ПО по 10-ю включительно).

Поэтому, если в аппарате указанная защита отсутствует, программа SST работает в режиме NORMAL (например, на рис. 3.16 показан соответствующий «флажок» 1 в окне Boot Mode). Если же защита есть, переводят «флажок» в положение 2 (Test-Point) и в этом режиме выполняют коммутацию указанного вывода процессора или других связанных с ним элементов до положительного решения проблемы.

Примечание. *Программа SST имеет очень полезное справочное окно, запускаемое следующим образом HELP — Test Point Information В нем показаны точки (и элементы) электронных плат различных моделей телефонов, на которые выведен описанный выше вывод процессора (например, для типов процессоров PMB 6850 и PMB 7850 — T9) Эти точки (элементы) показаны на фотографиях с различными пояснениями (правда, на английском языке) Все пояснения сортированы для различных моделей телефонов Внешний вид окна показан на рис 3 17*

Есть еще третий вариант «обхода» защиты. Большинство из рассматриваемых типов телефонов имеют режим поддержки Java-приложений (для сведения, JAVA — это универсальный язык для создания управляющих программ устройств различного назначения, в которые входят и сотовые телефоны). Переключив флажок в положение 3 (Java Patcher — см. рис. 3.16), с помощью JAVA-патчей модифицируется содержимое памяти телефона таким образом, что не опрашивается логическое состояние вывода Т9 процессора, вследствие чего «обходится» описанная выше защита

Для телефона «Siemens С55» этот патч состоит из двух файлов, называемых **px5amd.jad** и **px5amd.jar**. Механизм работы с ними следующий. С помощью программы Data Exchange Software, позволяющей работать с областью памяти CONTENT, в директорию JAVA телефона копируют эти два файла. После этого включают телефон, через его меню заходят в папку JAVA и запускают в ней приложение **px5amd** (в меню телефона отображается только один файл). После появления на дисплее телефона белого поля вводят пароль 39116. Затем на экране аппарата будут последовательно отображаться цифры от 0 до 9, и телефон после этого выключится.

Включают телефон, вновь запускают приложение **px5amd** и вводят тот же пароль (39116). После этого область загрузчика (Boot Core) телефона будет модифицирована и на экране аппарата появится сообщение «ALLREDY OK»

Далее запускают программу SST и работают с ней, как в обычном режиме (установив флажок 3, см рис 3.16) Этот вариант «обхода» защиты требует включения телефона и работы через его меню.

Следует отметить, что подобный механизм «обхода» защиты справедлив, если в телефоне используется Flash-память фирмы AMD.

В уже упоминавшемся окне программы SST (HELP) имеется инструкция по «обходу» защиты с помощью Java-приложений (см. строку 1 «Java

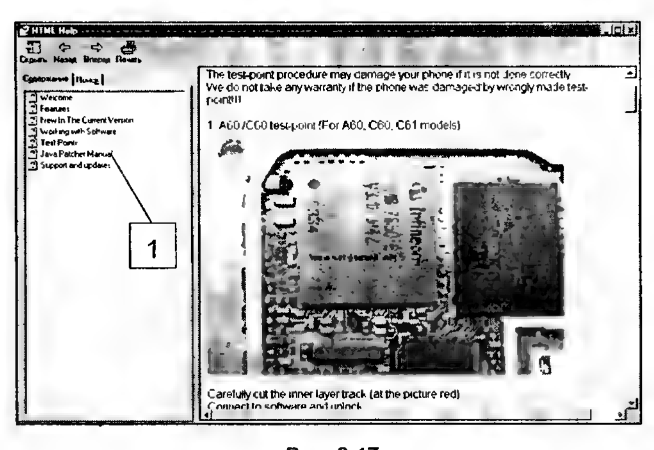


Рис. 3.17

Patcher Manual» на рис. 3.17). Из нее можно почерпнуть много интересного.

В заключение остановимся на назначении некоторых кнопок программы SST:

- кнопками 4 и 5 (рис. 3.16) открываются окна программы для телефонов EGOLG и SGOLG соответственно;
- кнопка 6 — калькулятор, с помощью которого вычисляются коды разблокировки телефонов по IMEI-номеру (только для моделей CT55 и SL50);
- кнопка 7 открывает окно регулировки контрастности дисплея. Как правило, эту операцию выполняют после замены дисплея аппарата или после перепрошивки файлом, считанным с другого телефона;
- кнопка 8 вызывает окно, с помощью которого можно выполнить калибровку аккумулятора. При необходимости, этот файл калибровки можно сохранить;
- кнопка 9 — запуск окна HELP.

Программа FREIA

Эта программа является самой популярной среди ремонтников сотовых телефонов.

Окно программы FREIA показано на рис. 3.18.

Остановимся на назначении ее некоторых кнопок.

Кнопка 1 «Read flash from phone» (рис. 3.18) открывает окно, показанное на рис. 3.19. Оно позволяет прочитать различные области Flash-памяти телефона (в том числе и заданные вручную) Это окно используется в основном для создания резервных копий Flash-памяти.

При выборе области памяти программа предлагает указать тип файла — выбирают формат FLS (см. рис. 3.20). Далее для выбранного файла указывают область памяти (например, Boot Core), куда его необходимо прошить.

Кнопка 2 «Unlocking functions»(рис. 3.18) открывает окно разблокировки (рис. 3.21).

Выбор («галочкой») первой строки на этом рисунке позволяет создавать LOG-файл из Flash-памяти телефона, а выбор второй — MAP-файл из LOG-файла (эти файлы необходимы для перезаписи области памяти блокировок телефона). Например, запись MAP-файла «поверх» исходной области EEPROM телефона позволяет снять блокировку телефона.

Выбор третьей строки позволяет создавать группы MAP-файлов из LOG-файлов, а четвертой — MAP-файлов непосредственно из Flash-памяти телефона

Выбор пятой строки обеспечивает включение режима разблокировки телефона (с сохранением резервной копии MAP), а шестой — включает разблокировку без создания резервной копии MAP Седьмая позволяет сохранить резервную копию MAP из телефона, а восьмая — загрузить MAP в телефон.

Остановимся на строке 6 подробнее. После ее выделения и нажатия кнопки ОК появится окно, показанное на рис. 3.22. Если телефон имеет OTP-область, нажимают кнопку «Use original IMEI» (использовать оригинальный IMEI). При

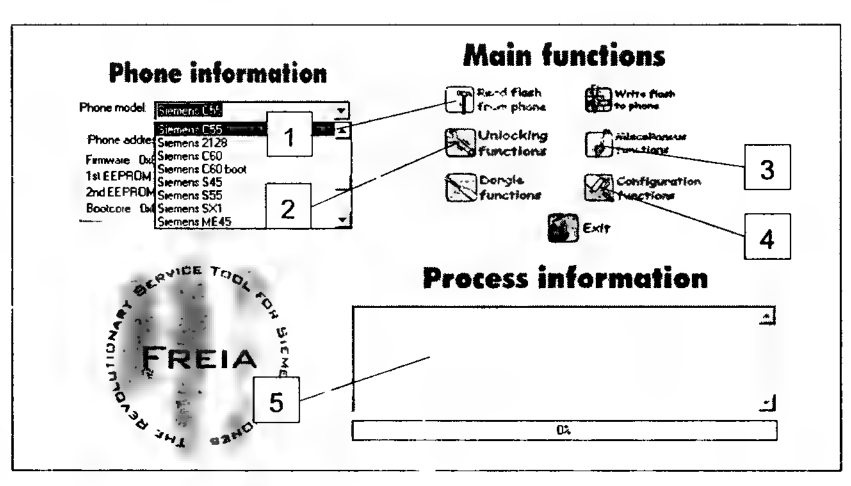


Рис. 3.18

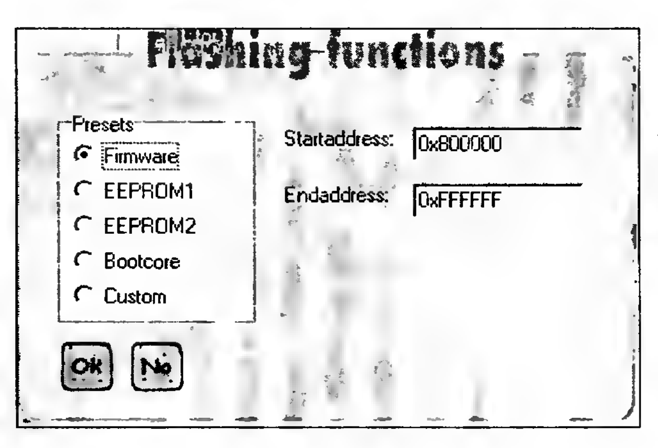


Рис 3.19

Рис. 3.22

этом IMEI-номер считывается из OTP-области телефона и записывается в EEPROM с пересчетом контрольных сумм и аппарат автоматически разблокируется

Если телефон не имеет OTP-область и необходимо изменить IMEI-номер аппарата, то нажимают кнопку «Use EEPROM IMEI» (в этом случае программа «переписывает» IMEI-номер из области EEPROM). Отметим, что эта функция не работает на аппаратах 55-й и 60-й серий В правой половине окна, поставив соответствующие «галочки» в окна 1 и 2, можно автоматически или вручную провести блокировку под оператора (провайдера)

«Галочка» 3 чаще всего используется, если в телефон была установлена новая микросхема Flash-памяти

Кнопка 3 «Miscellanous function» (рис 3 18) открывает окно, показанное на рис 3 23 В этом окне можно модифицировать («патчить») области Boot Core телефона (а не с помощью Java-патчей, как описывалось выше) Выбор второй строки окна позволяет «патчить» Boot Core в считанном FLS-файле содержащем Boot Core.

Третья строка позволяет считать и сохранить настройки аккумулятора, а четвертая — восстановить эти настройки

Кнопка 4 «Configuration function» (рис 3.18) открывает окно, показанное на рис. 3.24.

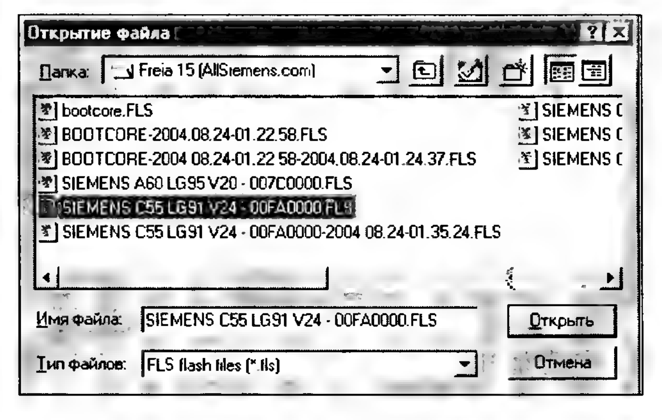


Рис. 3.20

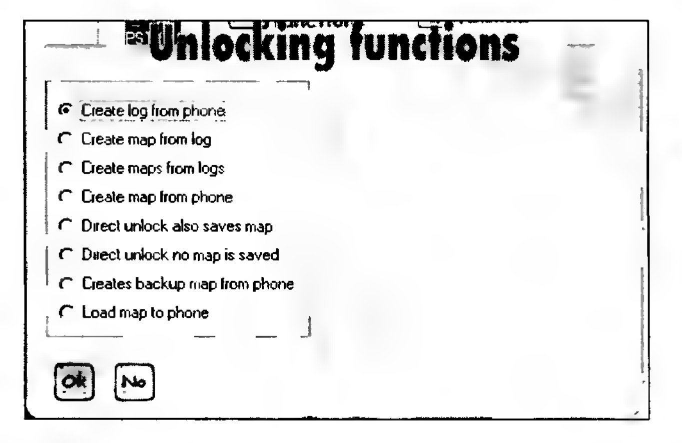


Рис 3.21

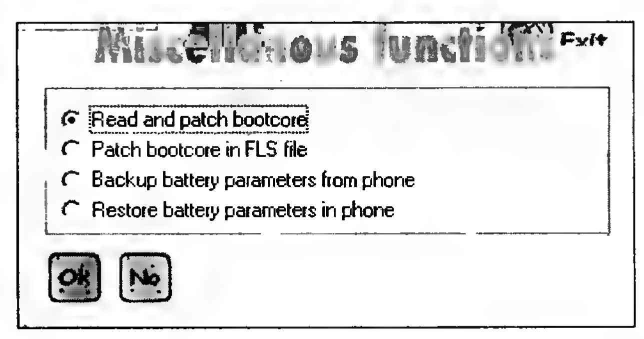


Рис. 3.23

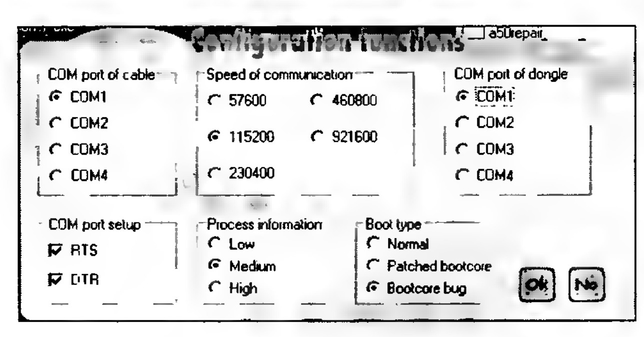


Рис. 3.24

После загрузки программы FREIA, именно это окно открывают в первую очередь и выполняют в нем необходимые настройки: выбирают номер COM-порта ПК, скорость обмена, «Boot type» (см. аналогичное окно в программе SST — «Boot Mode») и др.

В терминальном окне 5 (рис. 3.18) отображается процесс выполнения выбранного задания (например, как на рис. 3.25).

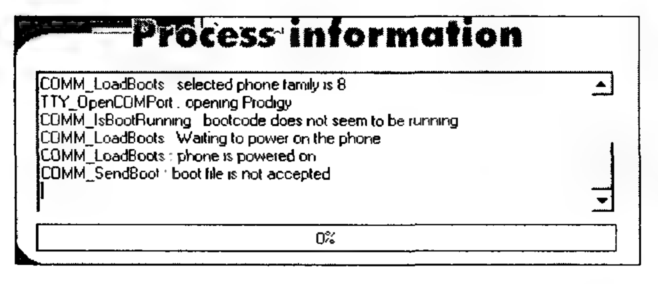


Рис. 3.25

В остальном, программа пояснений не требует.

Программа V KLAY

Программа V KLAY позволяет побайтно модифицировать область EEPROM (или ее выбранные части), самостоятельно создавать «патчи» и производить многие другие операции. Программа имеет дружественный русскоязычный интерфейс, позволяющий работать оператору по принципу «вопрос-ответ». Кроме того, она может работать с телефоном как бы в режиме конструктора, предусматривающего замену языка пользовательского интерфейса и шрифтов, изменение раскладки клавиатуры и картинок, отключение различных предупреждений и др. Последняя версия программы — V KLAY ver 2.7.

Внешний вид окна программы V KLAY показан на рис. 3.26.

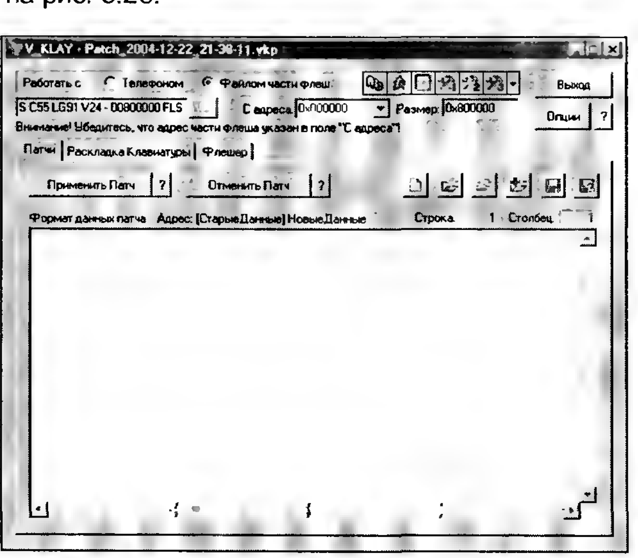


Рис. 3.26

Полезные программы для програмного ремонта телефонов SIEMENS

Siemens Contrast Tool

Программа Siemens Contrast Tool предназначена для регулировки контрастности дисплеев телефонов. Ее окно показано на рис. 3.27.

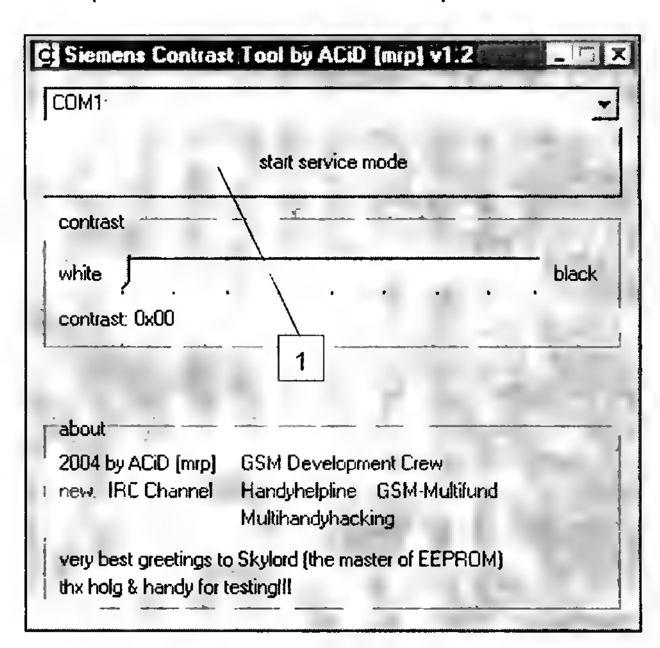


Рис. 3.27

Программа проста в настройке и в работе, поэтому развернутых пояснений не требует. Отметим лишь, что для регулировки контрастности дисплея телефон переводят в сервисный режим. Для этого нажимают кнопку 1 «Start service mode». В этом случае на экране телефона появится сообщение «SERVICE MODE».

Программа предназначена для телефонов SIEMENS как с цветными, так и с монохромными дисплеями.

Smelter

Эта программа используется в комплекте с программой V KLAY. Она дизассеблирует загруженный в нее файл Flash-памяти и на основе этого позволяет его модифицировать для различных целей. Программа имеет русскоязычный пользовательский интерфейс, позволяющий работать по принципу конструктора.

Окно программы Smelter показано на рис. 3.28.

Siemens Quick EEPROM Features

Программа «Siemens Quick EEPROM Features» подходит для моделей 45-й и 55-й серий.

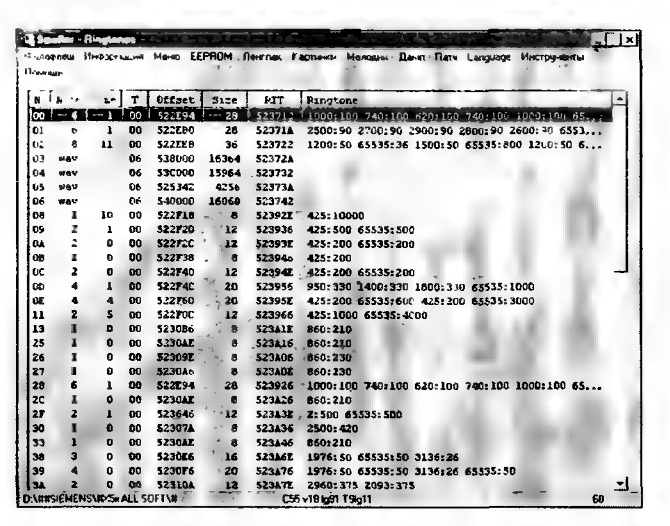


Рис. 3.28

Она позволяет включать или отключать некоторые функции телефона.

Программа выполняет некоторые функции V KLAY, но имеет значительно меньшие возможности. Ее окно показано на рис. 3.29.

Перечислим функции программы («галочка» означает включенное состояние):

- включение алгоритма шифрования речи (1 на рис. 3.29);
- коммутация режима подтверждения включения (2);
- активация дополнительных возможностей (3) пользовательского интерфейса (только для модели C55);
- ручное переключение поддиапазонов (4);
- снятие операторских настроек телефонов моделей S/ME45 и их установка, как для S45 (5);
- включение функции Java на модернизированных моделях телефонов SL42/45 (6).

Как вы знаете, телефоны производства фирмы SIEMENS получили во всем мире очень широкое распространение не только из-за их функций, но и из-за достаточно простого доступа к ПО этих телефонов, позволяющих модифицировать данный набор функций. В связи с этим в мире существует бесчисленное множество программ, позволяющих работать с ПО телефонов SIEMENS и рассказать обо всех программах не возможно, как невозможно вместить в рамки одной статьи даже самые основные из них. Мы обещаем продолжить рассказ о программах для работы с телефонами этого производителя в будущих номерах журнала.

Более подробно с информацией о процессорах фирмы Infineon, установленных в телефонах SIEMENS, можно ознакомиться на сайте производителя: http://www.infineon.com

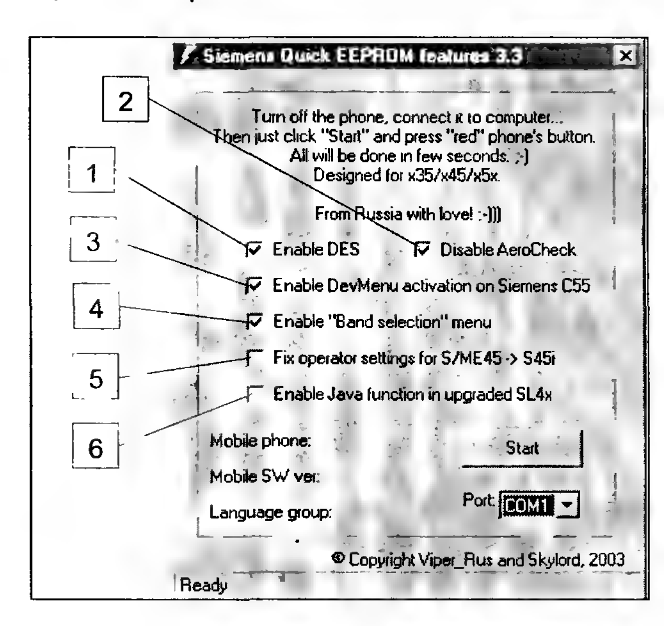


Рис. 3.29

Глава 4. Сотовые телефоны LG

Общие сведения

Одной из особенностей телефонов LG является то, что в них практически отсутствует программно-аппаратная защита. Все области памяти этих аппаратов, защищенные у других брендов (Nokia, Siemens и др.), доступны почти без ограничений для чтения и записи. При программировании телефонов желательно не модифицировать содержимое области загрузчика (BOOT) в Flash-памяти аппаратов, построенные на базе микропроцессоров фирмы TEXAS INSTRUMENTS. При повреждении данных в этой области телефон не «детектируется» компьютером через SERIAL INTERFACE и программирование телефона, как и восстановление BOOT области возможно только через аппаратный интерфейс JTAG.

Большинство моделей телефонов LG выполнены на процессорных комплектах от TEXAS INSTRUMENTS (TI) и ANALOG DEVICES (AD), в кторые входят центральный процессор, а также сигнальный процессор (DSP), аудио контроллер и контроллер питания. Некоторые перечисленные компоненты могут быть объединены в одном корпусе микросхемы, например, процессор и DSP (TI). На рис. 4.1 показаны печатные платы некоторых популярных аппаратов LG. Из него видно, что в 600 модели (1) используются комплекты на микросхемах TI (обведены контуром), а в моделях 510, G5220, G5300 и 3000 (2-5) — AD. В зависимости от производителя процессорных комплектов, программирование этих телефонов имеет свои особенности.

Отметим также, что при программировании телефонов LG необходимо постоянно держать

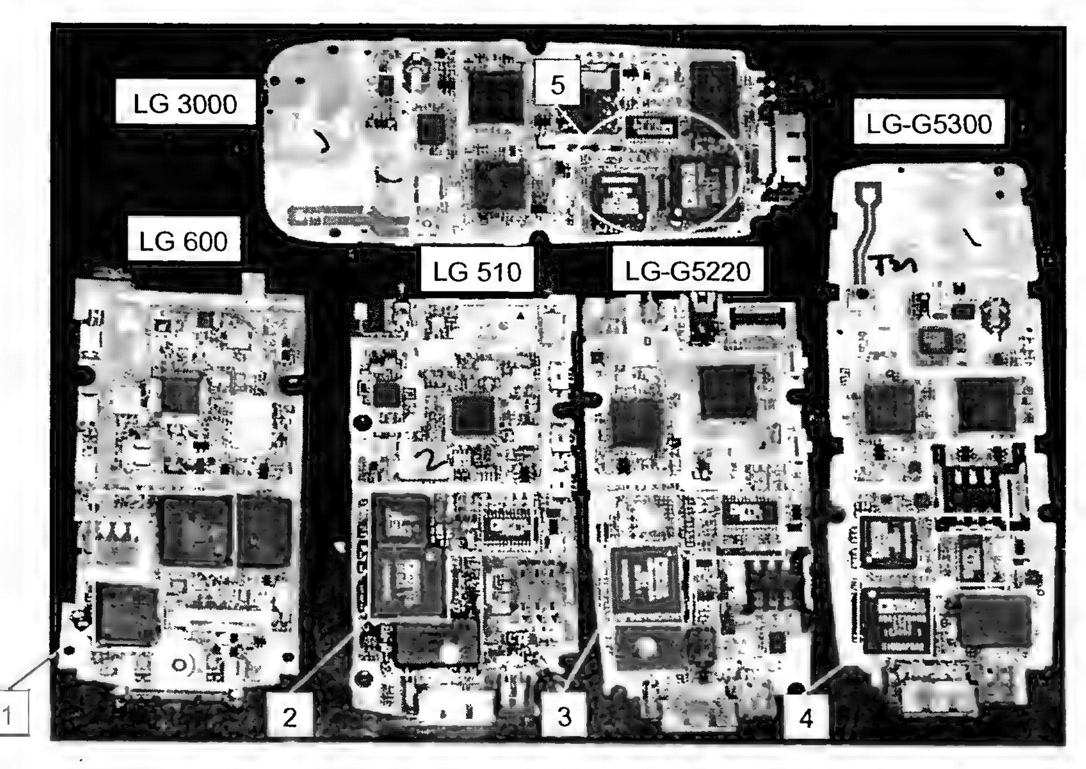
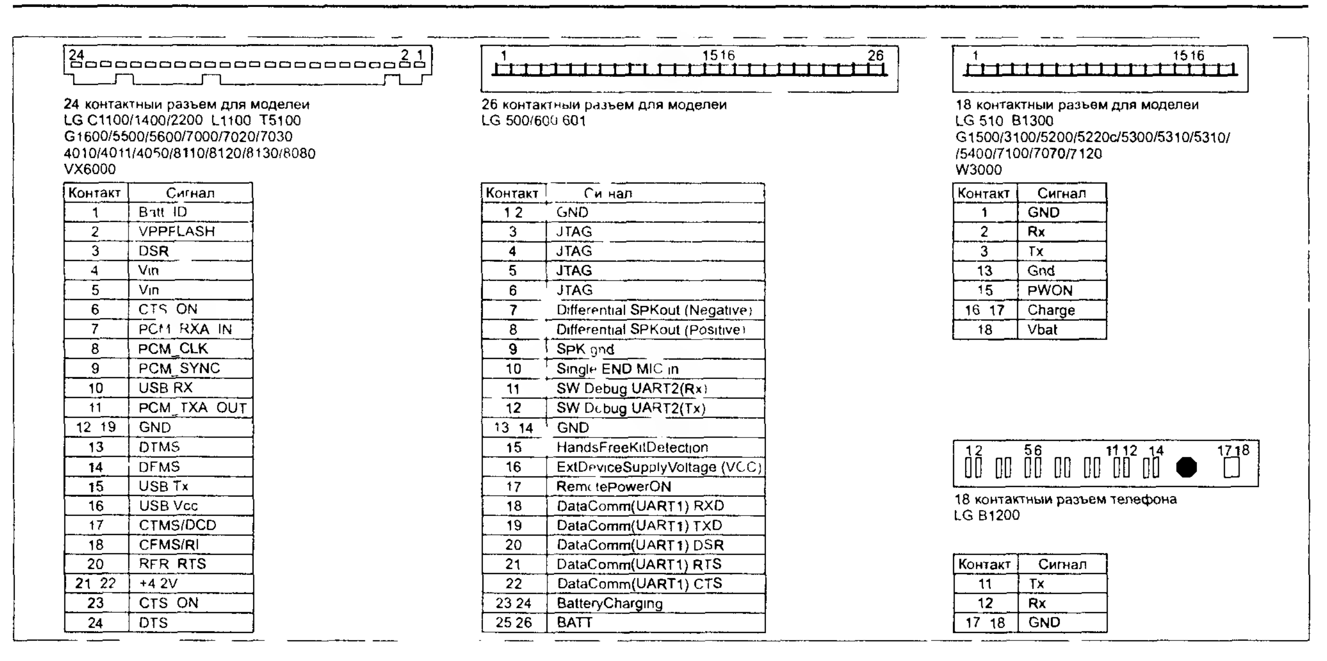


Рис. 4.1



Контакт	Сигнал
1	Batt ID
2	VPPFLASH
3	DSR
4	Vin
5	Vin
6	CTS ON
7	PCM RXA IN
8	PCM_CLK
9	PCM_SYNC
10	USB RX
11	PCM_TXA OUT
12 19	GND
13	DTMS
14	DFMS
15	USB Tx
16	USB Vcc
17	CTMS/DCD
18	CFMS/RI
20	RFR RTS
21 22	+4 2V
23	CTS ON
24	DTS

Контакт	Сигнал
1 2	GND
3	JTAG
4	JTAG
5	JTAG
6	JTAG
7	Differential SPKout (Negative)
8	Differential SPKout (Positive)
9	SpK gnd
10	Single END MIC in
11	SW Debug UART2(Rx)
12	SW Debug UART2(Tx)
13 14	GND
15	HandsFreeKitDetection
16	ExtDeviceSupplyVoltage (VCC)
17	RemotePowerON
18	DataComm(UART1) RXD
19	DataComm(UART1) TXD
20	DataComm(UART1) DSR
21	DataComm(UART1) RTS
22	DataComm(UART1) CTS
23 24	BatteryCharging
25 26	BATT

Контакт	Сигнал
1	GND
2	Rx
3	Tx
13	Gnd
15	PWON
16 17	Charge
18	Vbat

Контакт	Сигнал
11	Tx
12	Rx
17 18	GND

Рис 4.2

кнопку включения питания на передней панели телефона Для длительного нажатия указанной кнопки многие ремонтники используют специальные зажимы (или, например, струбцины) но намного удобнее, если сигнал POWER ON сервисного разъема соединить с общей шиной через малогабаритный переключатель или напрямую — тогда при подключении кабеля не будет необходимости держать клавишу включения нажатой

Назначение контактов разъемов некоторых моделей телефонов LG приведено на рис 4 2

Из этого рисунка также видно, что на некоторые телефоны можно подавать внешнее питание (Battery Charging) — в этом случае в процессе программирования аппарата аккумуляторную батарею можно снять

На рис 4 3 показана схема DATA-кабеля для связи COM-порта ПК и телефонов, имеющих 18-контактный разъем (модели 1300, G1500/ 3100/ 5200/ 5220c/ 5300/ 5310/ 5410/ 7100/ 7070/ 7120 и W3000)

Отметим, что модель телефона LG B1200 является аналогом телефона «Alcatel XG1», изменено лишь его ПО.

Программные пакеты для программирования телефонов LG

Для программирования телефонов LG существует несколько основных программ и очень много их разновидностей Остановимся на тех

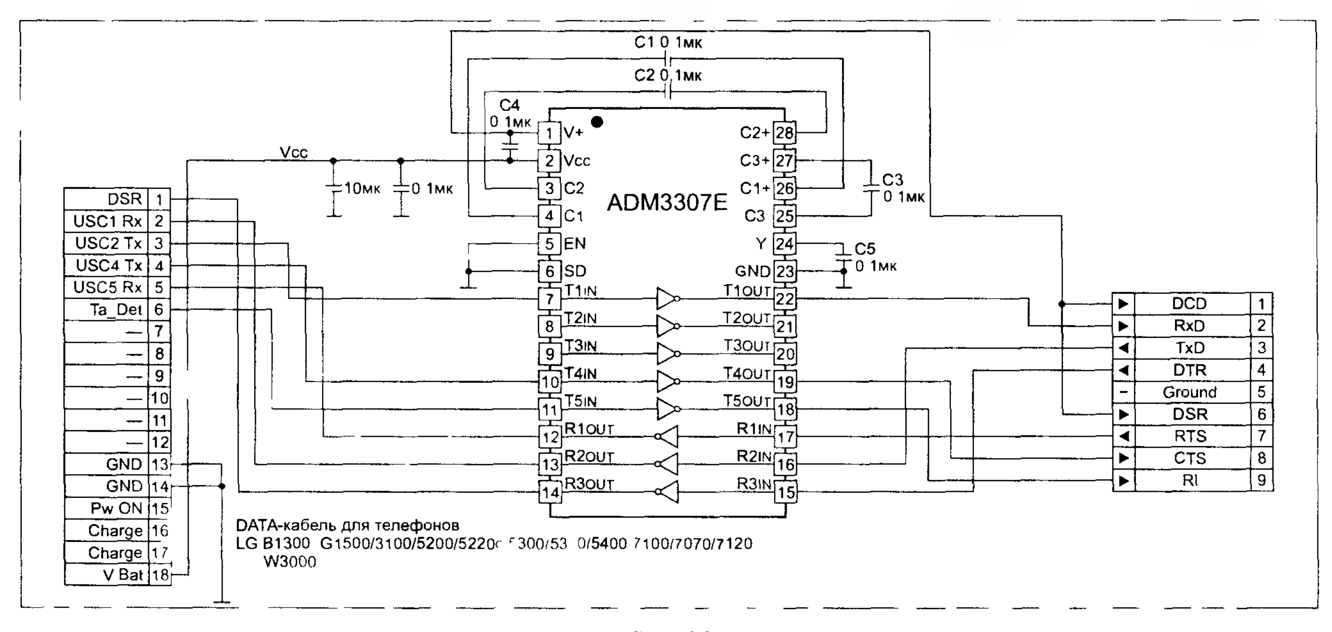


Рис 4.3

продуктах, которые имеются в свободном доступе (Интернет и др.).

Программа Floader

Окно программы Floader (ver 2.2) показано на рис. 4.4.

Эта программа позволяет выполнять все основные операции по чтению/записи/стиранию данных (ПО) в памяти телефона.

Первое, что необходимо сделать при работе с данной программой — это выбрать порт ПК и скорость обмена данными (в нашем случае — это СОМ-1 и 115200 бод, см. 1 на рис. 4 4). Затем считывают и сохраняют файл настроек телефона (настройки радиоканала, калибровки аккумулятора и др.), нажав закладку Read cal data (2) Кнопку «...» (3) нажимать не нужно, так как после этого в окне 4 будет предложено открыть уже записанный в памяти ПК файл настроек с расширением * bin В этом окне вручную прописывают путь, по которому будет считан этот файл из памяти телефона и записан на жесткий диск ПК (создана резервная копия файла настроек) Нажимают кнопку START — в окне информации 5 должна появиться надпись «Using embedet plpmon Power On/Reset Target». Нажимают и удерживают кнопку включения телефона (или выключатель на DATA-кабеле) до завершения чтения этого файла из телефона (этот процесс можно контролировать в окне 6 по нарастанию прогрессирующей шкалы). После появления в окне 5 сообщения «Reading completed» отпускают кнопку включения телефона. Операция чтения настроечного файла обычно длится около 20 с.

Если нужна резервная копия ПО телефона, выбирают закладку READ — 1 (рис. 4 5), прописывают путь в окне 2 и нажимают кнопку START. Дальнейшие действия описаны выше.

Следующим шагом выполняют операцию стирания старого ПО из Flash-памяти телефона — выбирают закладку ERASE (рис. 4.6) Затем в ниспадающем меню 1 выбирают модель телефона и нажимают START Дальнейшие действия аналогичны предыдущим шагам. В адресном окне ничего не нужно изменять, так как значения в нем устанавливаются автоматически, в зависимости от выбранной модели телефона.

После этого выбирают закладку Write (рис 4 7). Перед этим предварительно распаковывают архив с файлами прошивки (два файла с расширением * bif, а для других моделей могут быть расширения * m0 или *.mot) Нажимают в поле 1 Code_Flash1 (1 на рис 4.7) кнопку « ..» — после этого появится окно выбора файлов. В ниспадающем меню (тип файлов) выбирают Flash Binary Format (* bif) и находят папку с уже ранее распакованным архивом (с индексом 1 перед расширением bif) Ставят галочку в разделе

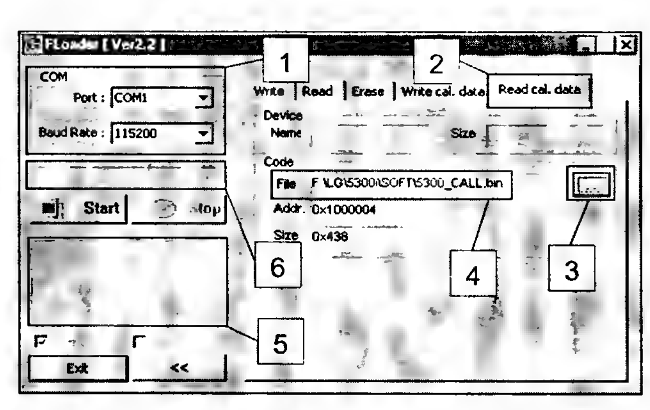


Рис. 4.4

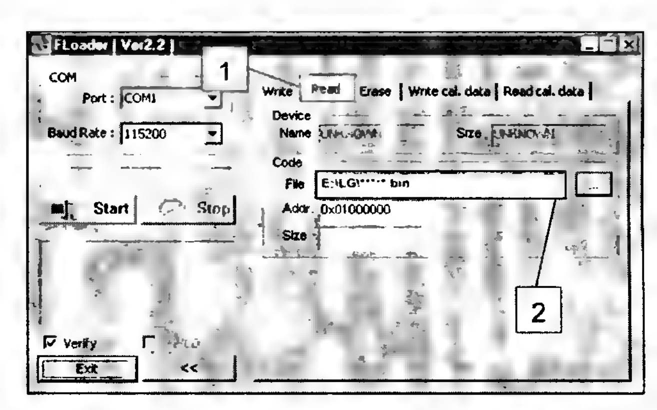


Рис. 4.5

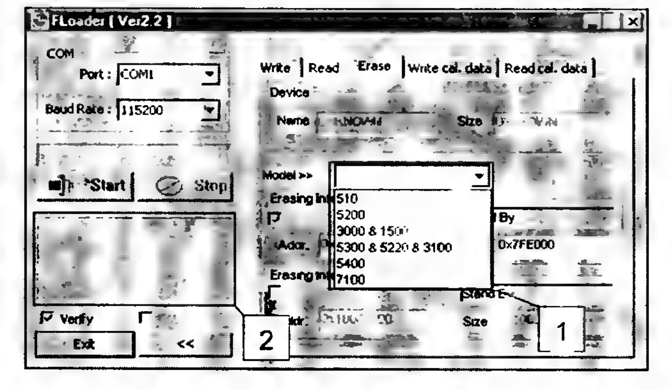


Рис. 4.6

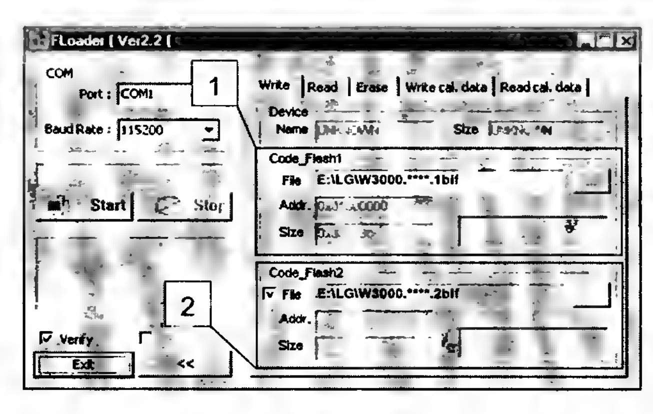


Рис. 4.7

2 Code_Flash2 и выбирают второй файл прошивки (с индексом 2 перед расширением) Нажимают кнопку START

Если в именах файлов прошивок отсутствуют индексы (1 или 2), можно использовать первый файл, в имени которого есть AlchemyData, а второй — CodeData

Затем нажимают кнопку START В процессе записи в окне сообщений последовательно появятся надписи Flash1 being Writing и Flash2 being Writing По окончании процесса записи файлов можно отжать кнопку включения телефона (выключить переключатель)

Заключительным шагом выбирают закладку Write cal data (рис 4 8) При выборе файла можно использовать файл настройки, уже предварительно сохраненный в процессе операции Read cal data

Но это еще не все — необходимо проверить работоспособность телефона после записи ПО и произвести его общий сброс на заводские установки

Включают телефон (процесс включения может занять до 30 с, но это происходит после первого включения — все последующие будут происходить быстро Затем на клавиатуре аппарата набирают следующую последовательность 2945#*# После этого появится инженерное меню (рис 4 9), в нем выбирают пункт FACTORY RESET (самая нижняя строка на рисунке — см 1) и сообщение о сбросе всех установок (рис 4 10) Кратковременно нажимают кнопку включения телефона (перезапускают аппарат)

В телефонах с поддержкой WAP, например, G5300 и G5300i, дополнительно в разделе «Интернет — PUSH-сообщения — Настроить» выбирают пункт ОТКЛЮЧИТЬ Затем нажимают кнопку включения телефона

Входят еще раз в инженерное меню (2945#*#), в пункте TRASE OPTION выбирают UART OFF и снова кратковременно нажимают кнопку включения телефона Это делается для избежания возможных проблем с синхронизацией телефона и ПК

Также в инженерном меню можно узнать текущую версию ПО телефона (пункт S/W VERSION)

Отметим что общий сброс телефона на заводские установки снимает пользовательский код (по умолчанию — 12345), а полное перепрограммирование ПО аппарата снимает операторскую блокировку

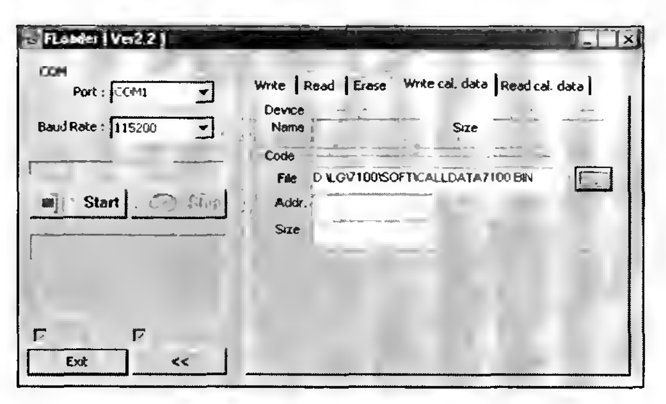


Рис. 4.8

Рис 4 9

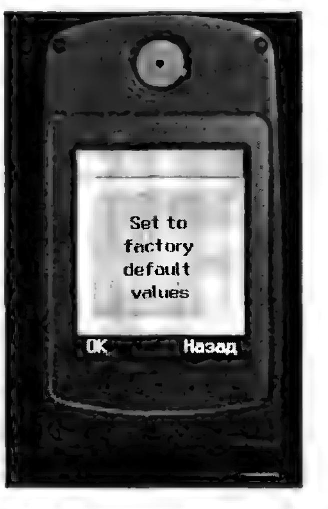


Рис 4.10

Программа FLUID (F.L.U.I.D.)

Программа FLUID — это заводской пакет, предназначенный для программирования телефонов, в которых используется процессорный комплект от TEXAS INSTRUMENTS На рис 4 11 показан процессор от TI — HERCROM200C телефона LG600 Этот комплект также используется

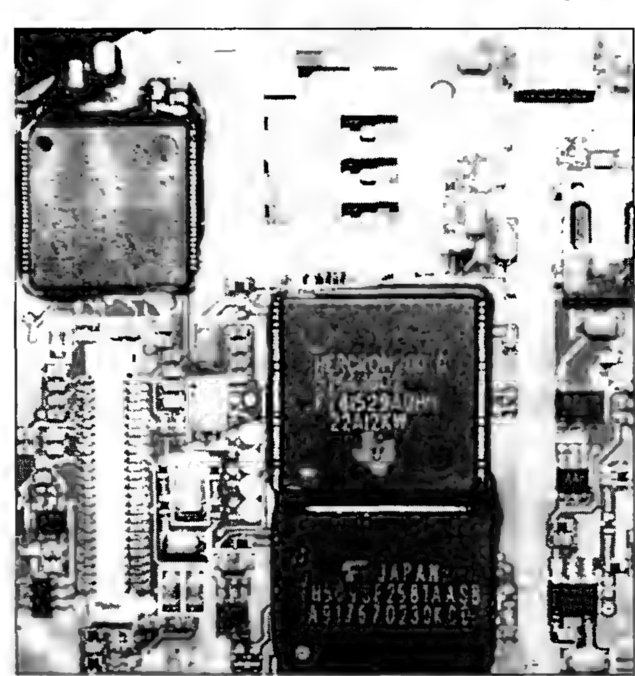


Рис 4 11

в телефонах 7000-серии Окно программы FLUID показано на рис 4 12.

Прежде чем начать работу с этой программой, ее необходимо настроить. в закладке GLOBAL SETTINGS в окне 1 выбирают тип процессора (это можно выяснить из его маркировки — см. рис. 4.11, или выбрать AUTO DETECT, для автоопределения), порт ПК (2) и скорость обмена (3).

Особенностью данной программы является то, что она работает в режиме командной строки. Чтобы выяснить, какие команды существуют, есть так называемый HELP — достаточно выбрать закладку OTHER FUNCTIONS (рис. 4.13), в нем выбрать пункт 1 и нажать EXECUTE (исполнить): в окне 2 (будет отображен весь список доступных команд. Окно 3 предназначено для команд. В этом же режиме, можно не использовать командную строку — достаточно выбрать опцию 4, но в этом случае программироваться будет вся область Flash-памяти телефона, за исключением загрузчика.

Следующим шагом выбирают закладку READ FLASH (рис. 4.14) — это необходимо для чтения и создания резервной копии содержимого **Flash**-памяти телефона, а в командной строке указывают путь для сохранения этого файла.

Затем выбирают закладку ERASE/PROGRAM FLASH (рис 4.15). В окне 1 выбирают путь к файлу прошивки, флажок в окне означает, что можно проверить в тестовом режиме наличие связи между телефоном и ПК (без стирания и записи памяти). Флажок 3 включает режим полного стирания Flash-памяти телефона (с настройками), а флажок 4 запрещает стирание и программирование загрузочной области памяти. Последний режим желательно активировать всегда, так как при сбоях программирования или других ошибках всегда останется «живой» загрузчик. Если программа-загрузчик по тем или иным причинам запорчена, восстановить ее можно только специальным программатором, использующий интерфейс JTAG.

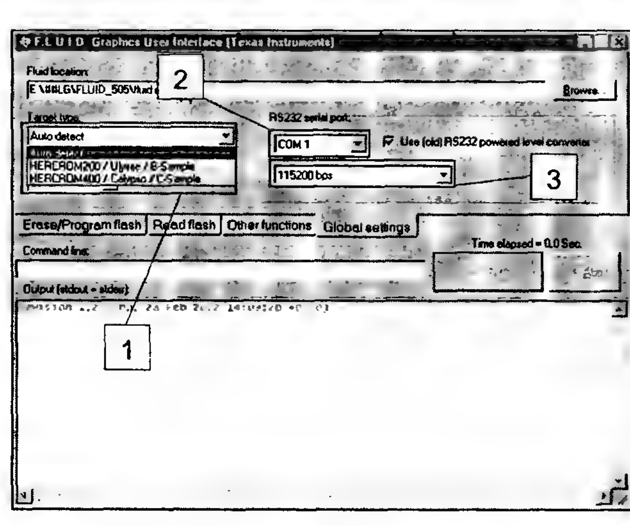


Рис. 4.12

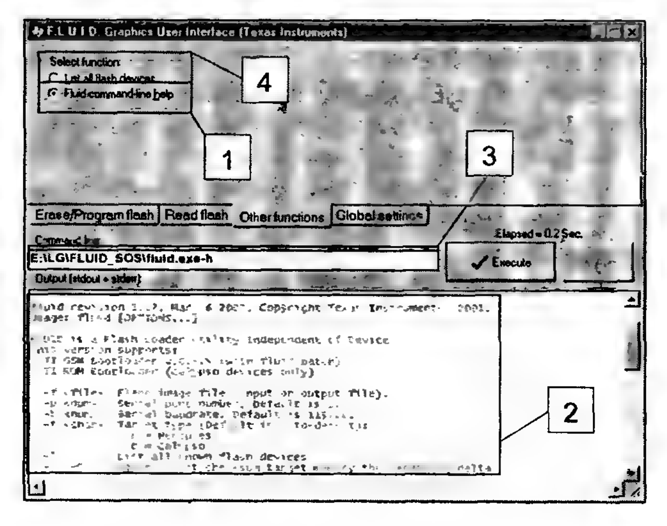


Рис. 4.13

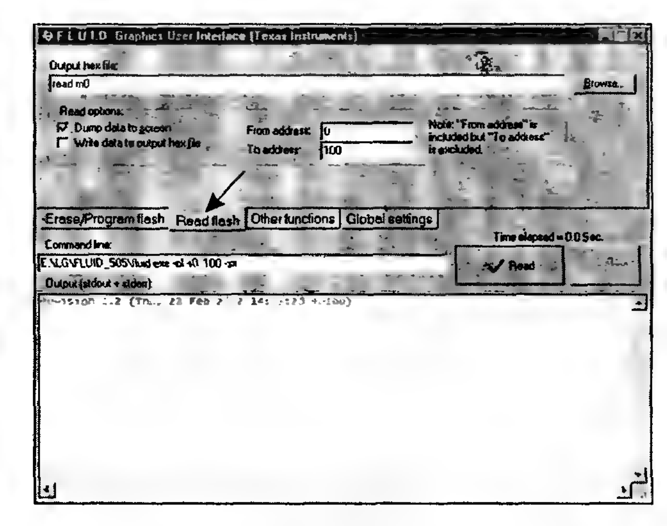


Рис. 4.14

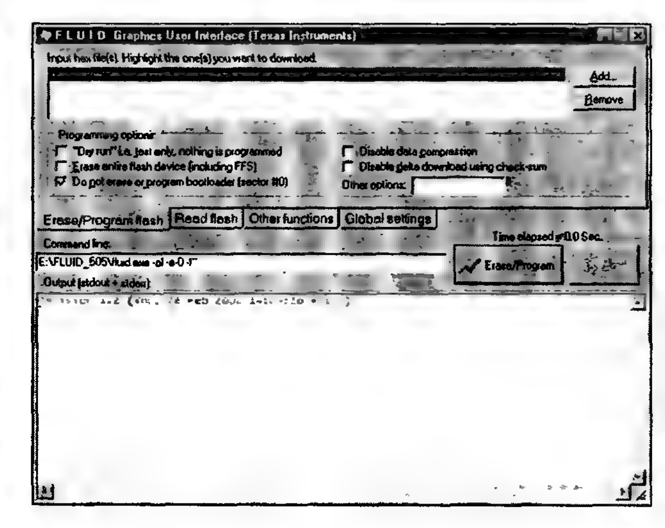


Рис. 4.15

Программа Monitor

Пакет MONITOR построен по принципу терминальной программы, его окно показано на рис. 4.16.

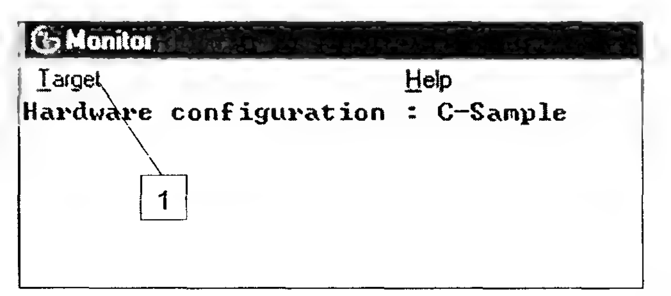


Рис. 4.16

В закладке TARGET (1) можно выбрать режимы конфигурации, связи (connect/disconnect) и синхронизации В меню конфигурации (см рис. 4.17) выбирают тип процессора, но позиции в нем несколько иные — это так называемые «служебные» названия: A/B/C-Sample (например, процессору HERCROM200 соответствует позиция B-Sample, а HERCROM400 — C-Sample).

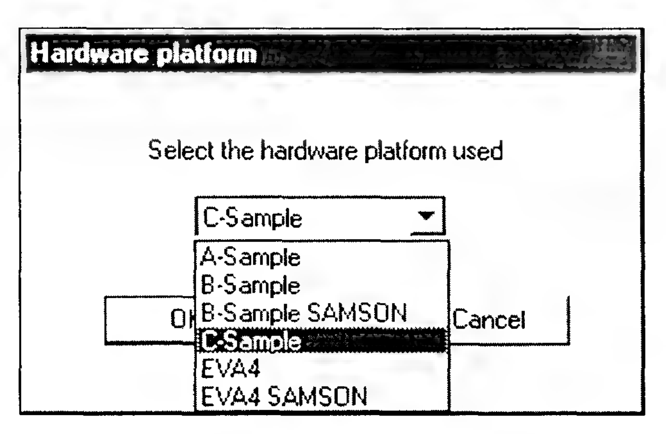


Рис. 4.17

При выборе «Target — Connect» выбирают COM-порт (и нажимают ОК), после чего нажимают и удерживают кнопку включения телефона. После этого на экране появится окно, показанное на рис 4.18. Из него можно узнать: тип процессора (C-Sample), запуск программы-загрузчика и ее версию (Version 6.1), загрузку программы-монитора в память (и контрольные суммы — 6859) и версию FlashLoader (Ver 6.6.3).

При нажатии закладки Flash (рис. 4.19) появляется меню, позиции которого означают:

- Get type — проверка типа Flash-памяти;
- Erase First Memory — выборочное стирание памяти;
- Erase Memory All — полное стирание памяти;
- Erase and Program Appli Only — стереть и запрограммировать Flash без области загрузчика;

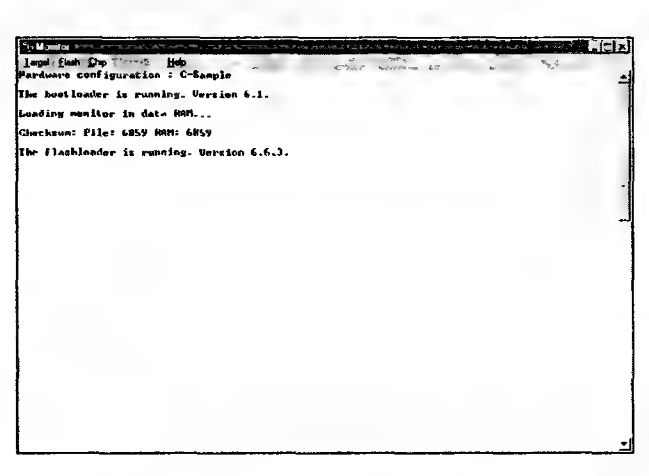


Рис. 4.18

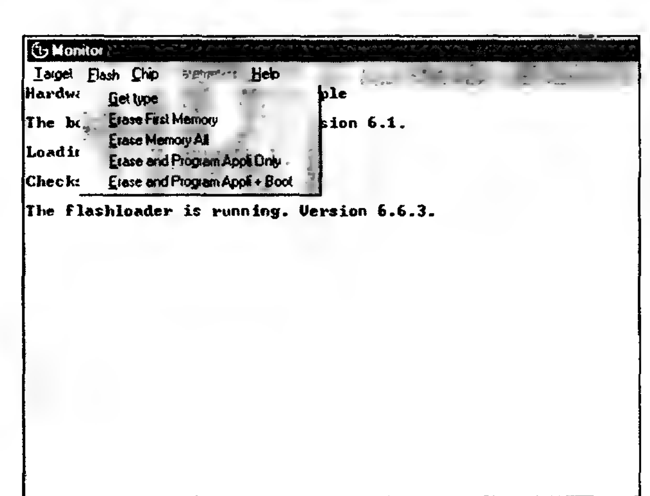


Рис. 4.19

- Erase and Program Appli + Boot — стереть и запрограммировать Flash с областью загрузчика.

Эта программа достаточно проста и далее комментариев не требует.

Программа MULTI (GSMMULTI)

Особенностью этого пакета является то, что он позволяет программировать телефоны как на процессорах TEXAS INSTRUMENTS, так и ANALOG DEVICES. Выбор программируемой модели телефона происходит из поставляемого в составе программы архива библиотек.

Программа не всегда корректно работает под ОС Windows XP (особенно с Servicepack 2). Поэтому ее лучше всего использовать с ОС Windows 98/2000.

Окно программы с меню конфигурации показано на рис. 4.20.

В строке DLL (1) после нажатия кнопки «...» (2) необходимо указать путь к файлу с расширением *.dll и названием модели программируемого телефона. Аналогично поступают в строке BIN (3) — выбирают файлы с расширением *.mot или *.m0. Если файлов прошивки два, например, *Al-

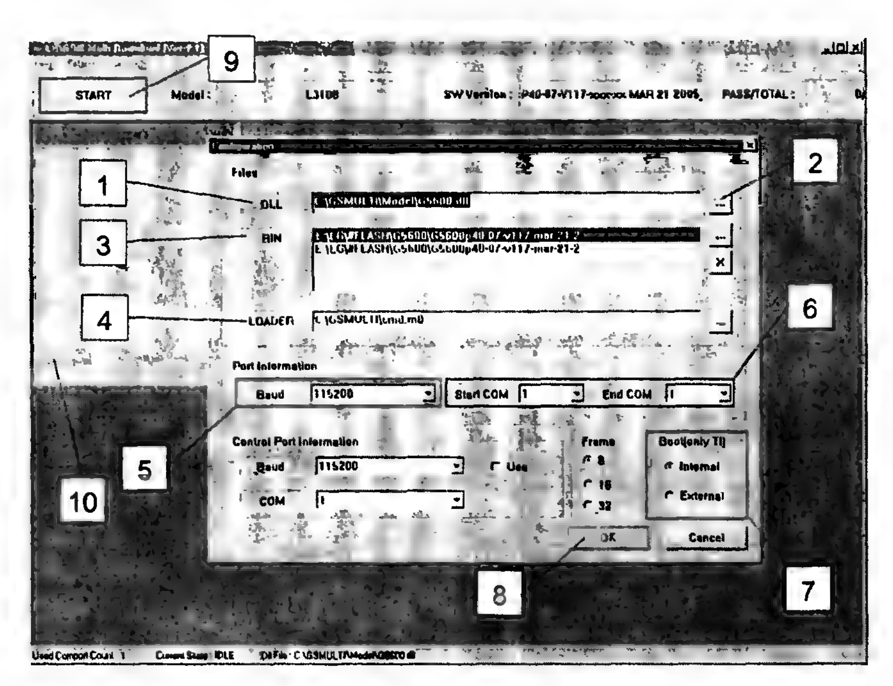


Рис. 4.20

chemy Data.mot и *Code Data.mot, то они устанавливаются поочередно.

В строке LOADER (4) аналогичным образом указывают нахождение файла загрузчика (устанавливается по умолчанию). Затем устанавливают скорость обмена (5) и номер порта ПК (6) — выбирают один и тот де номер порта в двух окнах.

Для всех моделей телефонов, в которых используется процессор ANALOG DEVICES, в группе BOOT (only TI — только для TEXAS INSTRUMENTS) необходимо оставить включенной позицию INTERNAL (7 на рис. 4.20). Затем нажимают кнопку ОК (8).

Перед программированием аппарата подключают к нему кабель, после чего нажимают кнопку START (8). После появлении сообщения Wait phone connecting нажимают кнопку включения телефона и удерживают ее на все время «прошивки» аппарата. О ходе процесса программирования в окне 9 будут появляться соответствующие сообщения. После завершения программирования отсоединяют кабель и включают телефон (процесс первого включения аппарата может быть довольно длительным — около минуты).

Если процесс включения телефона прошел нормально (на экране не появилась сообщение об ошибке FAIL), на клавиатуре аппарата набирают следующую последовательность: 2945#*#. После этого появления инженерного меню, проверяют в нем версию ПО аппарата, а также в пункте TRASE OPTION (в тех телефонах, где он есть) активируют строку UART OFF. Это делается для избежания возможных проблем с синхронизацией телефона и ПК (и не забывают про FACTORY RESET).

Программы разблокировки телефонов, программные калькуляторы и другие программы

Уже ранее отмечалось, что после прошивки нового ПО код блокировки (или операторская блокировка) снимаются.

Существует много программ, с помощью которых можно разблокировать телефоны LG, пользовательский интерфейс у них прост, поэтому останавливаться подробно на их описании нет смысла. Также существуют так называемые программы-калькуляторы, которые позволяют вычислить код блокировки телефона по его IMEI-номеру. Перечислим некоторые из этих программ:

- программа разблокировки телефона LG B1200 (ALCATEL XG1) — см. рис. 4.21;
- калькулятор для телефонов LG C1100/1200 и 3100 — см. рис. 4.22;

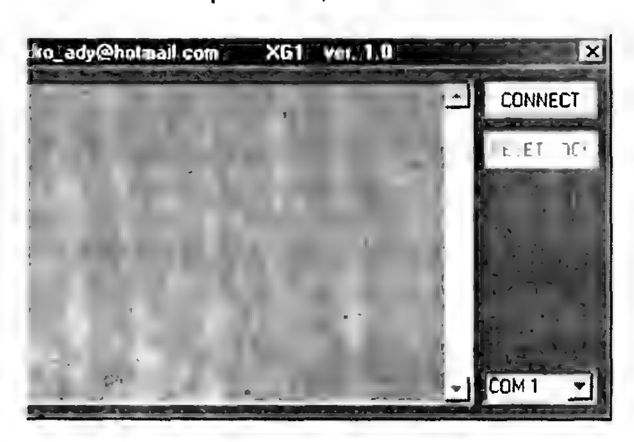


Рис. 4.21

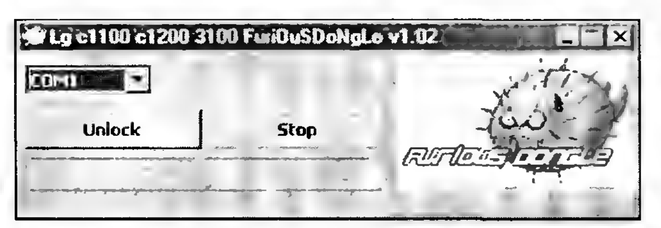


Рис. 4.22

- калькулятор для телефона LG 7020 — см. рис. 4.23;

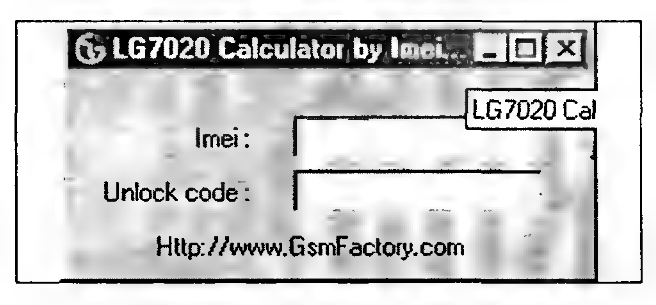


Рис. 4.23

- калькулятор для телефонов LG B1200 и 510W — см. рис. 4.24;

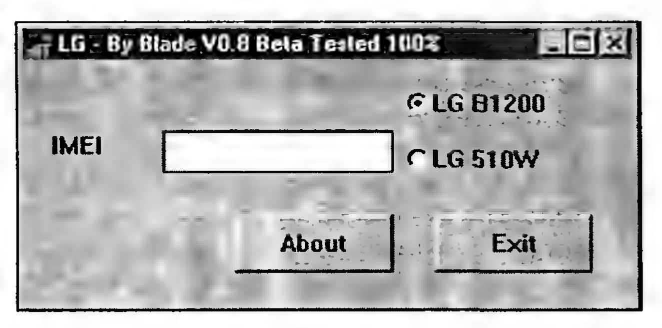


Рис. 4.24

- калькулятор для телефонов LG 510/1200/7020 — см. рис. 4.25;

Рис. 4.25

- программа разблокировки для телефонов LG U8110/8120 — см рис 4 26

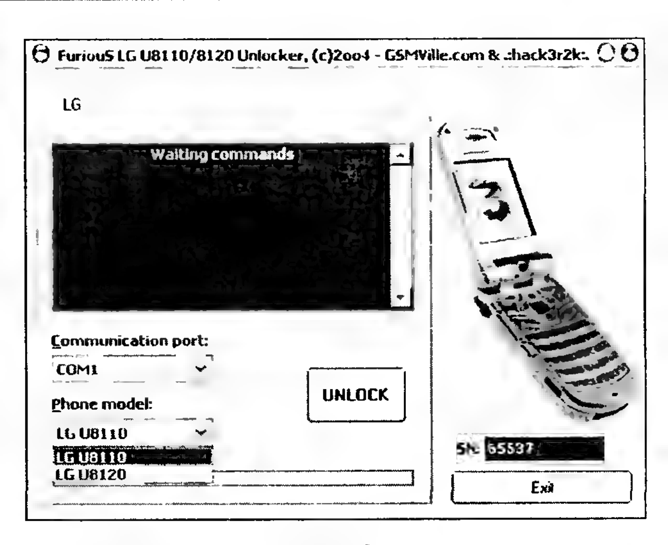


Рис. 4.26

Программа редактирования настроек телефона CALL_DATA

Эта программа позволяет редактировать «тонкие» настройки телефона усиление радиоканала (по поддиапазонам и каналам), калибровку опорных генераторов, аккумулятора, его температурного датчика и др. Ее окно показано на рис. 4.27. К этой программе поставляется также специальный пакет, который при наличии GSM-тестера позволяет как автоматически, так и вручную калибровать радиоканал телефона.

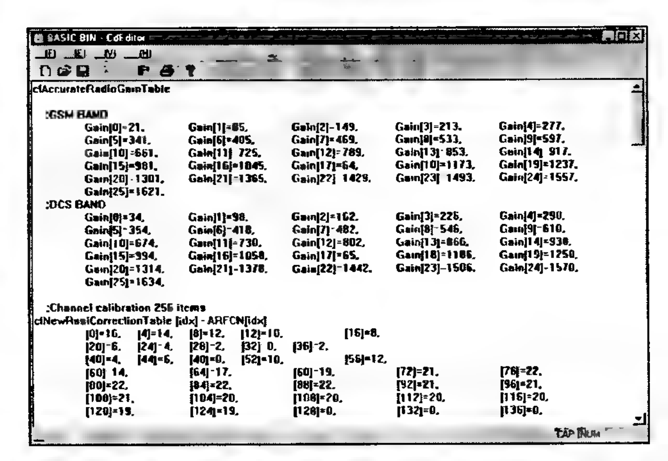


Рис. 4.27

Программа восстановления IMEI-номера IMEI FOR SVC

Окно этой программы показано на рис 4 28 В этом пакете при смене модели (1 на рис 4 29) автоматически меняется префикс серийного номера аппарата (IMEI-номера) 2 Оператору достаточно выбрать модель аппарата, ввести SERIAL NO (3) и CHECK BIT (4), который можно считать на задней крышке аппарата

Пакет позволяет читать оригинальный IMEI и версию ПО, проводить сброс настроек телефона (аналогично сбросу настроек через инженерное меню — см выше) и др

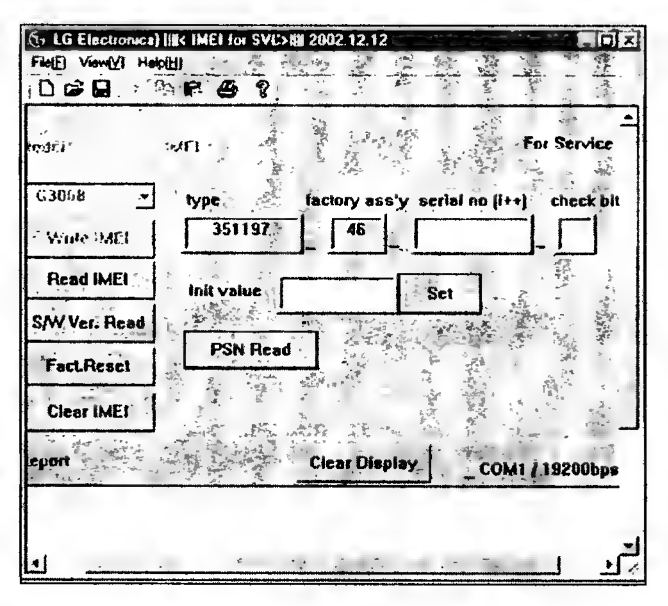


Рис. 4.28

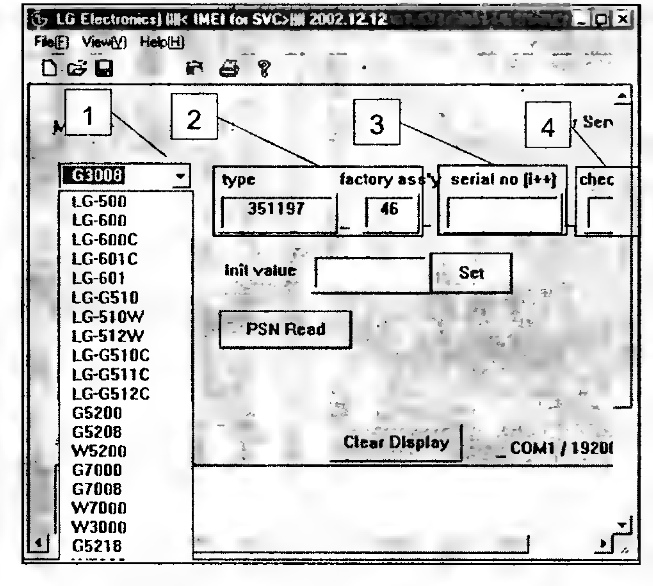


Рис. 4.29

Программа-автокалибровщик AUTOCAL

Окно загрузки этой программы показано на рис. 4 30. Она предназначена для точной калибровки узлов телефона. Кроме того, программа позволяет считывать и модифицировать калибровочные файлы, IMEI и др. Для правильной работы с данной программой необходим GSM-тестер.

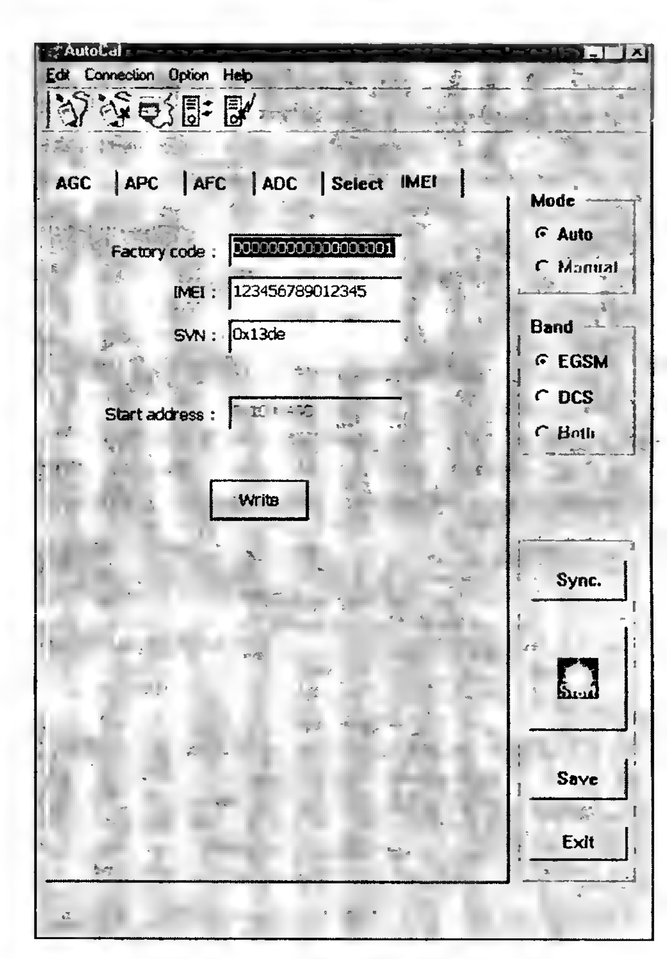


Рис. 4.30

Глава 5. Сотовые телефоны MOTOROLA

Модели: «Motorola T190/191»

Сотовые телефоны «Motorola T190/191» выпускаются компанией BENQ на так называемой платформе ACER — маркировка платы приведена на рис. 5.1. Внешне очень похожие модели T190/T191 (рис. 5.2) отличаются, в основном, только своими функциональными возможностями. Их основное аппаратное отличие заключается в том, что в модель T191 установлена отдельная микросхема оперативной памяти (RAM). Еще одной особенностью телефонов этих моделей является наличие микросхемы центрального процессора, включающей в себя сигнальный процессор (DSP). Также отметим, что на рынке представлены телефоны «Motorola T190» на платформе ZEUS китайского производства — этот телефон предназначен для китайского рынка и содержит микросхему флэш памяти вдвое меньшего объема, чем у остальных моделей.

Примечание: *BOOT — загрузчик представляет собой специальную программу, которая размащается в памяти процессора или в отдельной микросхеме FLASH-памяти Она позволяет производить процессору запись/чтение данных из памяти.*

LOADER— это специальная программа, загружаемая в процессор телефона из ПК. Позволяет компьютеру производить чтение/ запись данных флэш-памяти напрямую, используя процессор телефоне только как своеобразный программатор Для различных типов флэш-памяти программа LOADER саоя.

Программа-загрузчик (BOOT) в телефонах «Motorola T190/191», как и все ПО записана в отдельной микросхеме флэш-памяти (FLASH), а не в памяти процессора (в отличие от многих аппаратов других производителей). Это необходимо учесть ремонтникам, так как восстановление области BOOT в этих аппаратах возможно только при наличии отдельного программатора или отладочного интерфейса J-TAG, контакты для подключения которого выведены на плату телефона. В последнем случае необходимо специальное дорогостоящее оборудование и ПО.

Аппаратная структура рассматриваемых моделей почти ничем не отличается от телефонов «Panasonic GD90/92».

Снятие пользовательской блокировки

О видах блокировок и, конкретно — о пользовательской, подробно рассматривалось в главе 1.

Пользовательскую блокировку (USER LOCK или PHONE CODE) в телефонах «Motorola T190/191» (не путать с операторской блокировкой) можно снять без использования ПК и DATA-кабеля — для этого необходимо ввести специальный мастер-код. Этот код не позволяет определить «забытый» код доступа, но с его помощью можно получить доступ к функциям телефона. Мастер-код подходит ко всем аппаратам указанный моделей.

Остановимся на этой операции более подробно.

Устанавливают в телефон SIM-карту и включают его. После этого на экране появится сообщение, запрашивающее код телефона (если нет запроса PIN-кода). Набирают код 19980722 и затем нажимают зеленую кнопку OK (показана стрелкой на рис. 5.2). После подтверждения кода телефон разблокируется.

Однако, при следующем включении, телефон опять потребует ввода кода. Чтобы в дальнейшем этого не происходило, производят общий сброс настроек аппарата на заводские установки. Для этого включают телефон, вводят универсальный мастер-код (или UNLOCK-код), как было описано выше. Затем в меню телефона выбирают опцию ЗАЩИТА (SECURITY). В ней набирают еще один универсальный мастер-код (USER UNLOCK-код) — 20010903, и подтверждают его

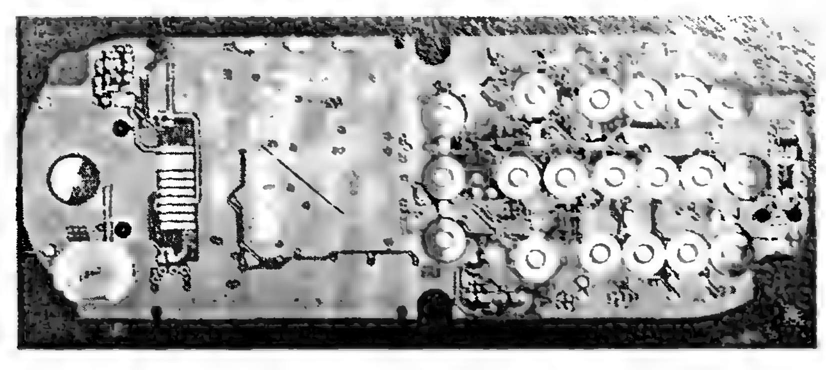


Рис. 5.1

Рис. 5.2

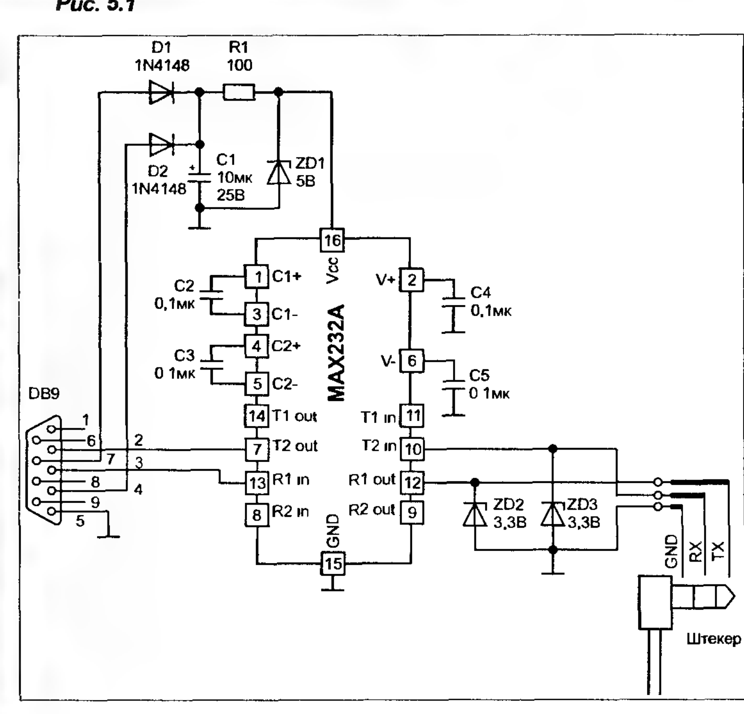


Рис. 5.3

ввод кнопкой ОК. После этого в аппарате будет произведен общий сброс всех настроек на заводские установки. При желании заново выполняют все пользовательские настройки телефона.

На некоторых версиях ПО телефона достаточно использовать только один из приведенных кодов.

Сброс настроек телефона до заводских установок выполняют также в следующих случаях:

— сбои аппарата, которые вызывают проблемы при работе с исходящими или входящими вызовами;
— некорректная работа аппарата при доступе к различным опциям меню.

Если же снятие пользовательской блокировки указанным способом выполнить не удалось, эту операцию выполняют с помощью ПК через DATA-кабель. Принципиальная схема одного из вариантов кабеля приведена на рис. 5.3. Соединитель DATA-кабеля вставляется в разъем телефона для подключения внешней гарнитуры (HANDS FREE), как показано на рис 5.4.

Примечание. *При работе с ПК аккумуляторная батарея (АКБ) телефона должна быть полностью заряжена!*

Существует несколько программ для ПК, с помощью которых можно снять пользовательскую блокировку или сделать полный сброс EEPROM аппаратов «Motorola T190/191», при котором USER LOCK-код снимается автоматически. Остановимся на одной из них — T19x TESTMODE (рис. 5.5).

Последовательность операций при работе с этой программой следующая:

— подключают выключенный аппарат через DATA-кабель к ПК;
— запускают программу на ПК;
— в окне программы нажимают кнопку RESET (1 на рис. 5.5);

Рис. 5.4

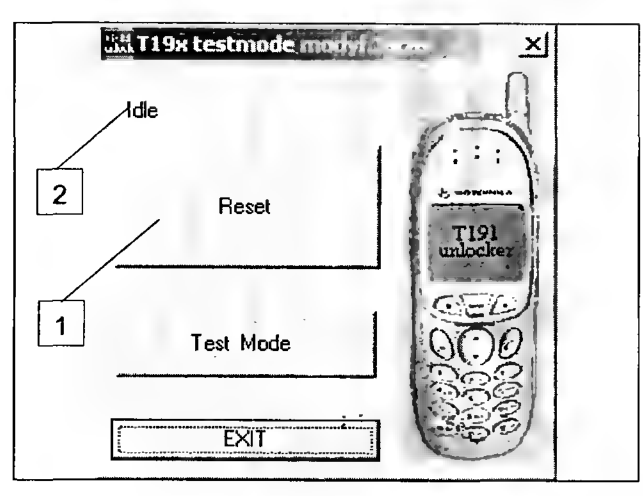


Рис. 5.5

- после этого программа выдаст сообщение, требующее включения телефона (в окне 2 появится сообщение «POWER UP PHONE»),
- кратковременно нажимают кнопку включения телефона;
- через некоторое время в окне 2 появится сообщение «IDLE», а из телефона должен быть слышен двойной короткий звуковой сигнал Это означает, что операция общего сброса телефона проведена успешно.

Таким образом можно исправить мелкие проблемы и «зависания», связанные с работой телефона

Рассмотрим характерные неисправности ПО телефонов «Motorola T190/191» и способы их устранения.

Характерные неисправности телефонов и способы их устранения

Телефон не включается (связь с ПК через DATA-кабель есть), его аппаратная часть исправна и область загрузчика (BOOT) не повреждена

В этом случае можно предположить, что неисправно ПО телефона. Чтобы его перезаписать, необходимо определить версию ПО, а также тип микросхемы FLASH-памяти, установленной в телефон.

Версию ПО можно определить, разобрав сам телефон Снимают заднюю крышку телефона, на экранной пластине имеется стикер (1 и 2 на рис. 5 6) Цифра 1 соответствует модели T190, а цифра 2 — T191

Версию ПО определяют следующим образом Например, на стикере 1 нанесена маркировка 101D3_5 87/20, а на 2 — MH117811 Это означает, что в первом случае версия ПО — 5 87, а во втором — 1 78

На рис 2 7 показано расположение микросхемы FLASH-памяти у различных моделей (1 — T191, 2 — T190

Тип микросхем FLASH-памяти определяют по маркировке на их корпусе Зная маркировку микросхемы FLASH-памяти, тип телефона и версию текущего ПО, можно определить, какую версию можно записать (такую же или обновленную).

Маркировка FLASH-памяти 28F320J3 (1 на рис. 5.7) телефона «Motorola T191» предполагает установку версий ПО от 7-й, а F160C3TC (2 на рис 5 7) — от 1-й («Motorola T190»).

Следует отметить, что комбинация последних букв (например, как в первом случае — J3) означает программный тип FLASH-памяти, который также требует соответствующую прошивку. Например, если на микросхеме обозначено T3, то уже требуется другой тип прошивки (для типа T3) Более подробно с этой информацией можно ознакомиться в сервисной документации на указанные аппараты.

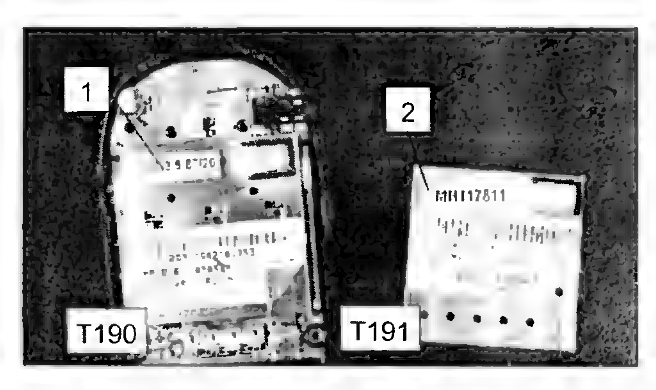


Рис. 5.6

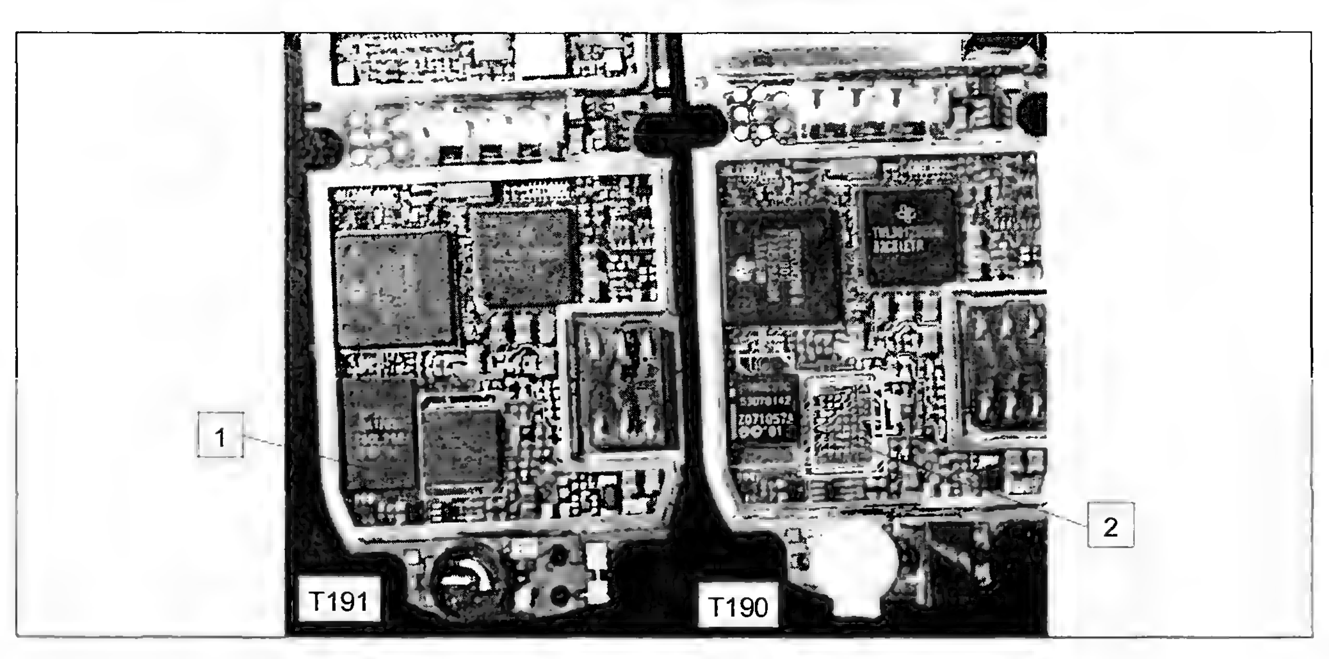


Рис 5 7

После определения версии ПО и соответствия ее тому или иному типу флэш-памяти, приступают к процессу перезаписи

Оригинальное (заводское) программное обеспечение на ПК для прошивки указанных моделей (платформа ACER) называется SERVICE DMTOOL Желательно использовать версию этой программы 3 15 (рис 5 8)

В качестве примера рассмотрим порядок прошивки ПО для телефона «Motorola T191», серии MH (стикер 2 на рис 5 6), версия прошивки 1 78

После загрузки программы нажимают кнопку MH (1 на рис 5 8), затем — кнопку BOOT FILE (2 на рис 5 8), выбирают путь к файлу загрузчика (LOADER) (r_flash_007 mot) и нажимают ОТКРЫТЬ (рис 5 9) Затем нажимают FLASH FILE (3 на рис 5 8) и аналогичным образом выбирают файл прошивки (MH117811 MOT) и опять нажимают ОТКРЫТЬ (рис 5 10)

Подключают выключенный аппарат через DATA-кабель к ПК и нажимают кнопку DOWNLOAD (4 на рис 5 8) После этого в окне 1 (рис 5 11) появляется сообщение о конвертировании файла прошивки и ожидания запуска процесса записи После появления в этом окне сообщения «Wait For Target Ready», кратковременно нажимают кнопку включения телефона

Затем будет выполняться операция записи ПО во FLASH-память телефона, в процессе которой появится индикатор копирования 1

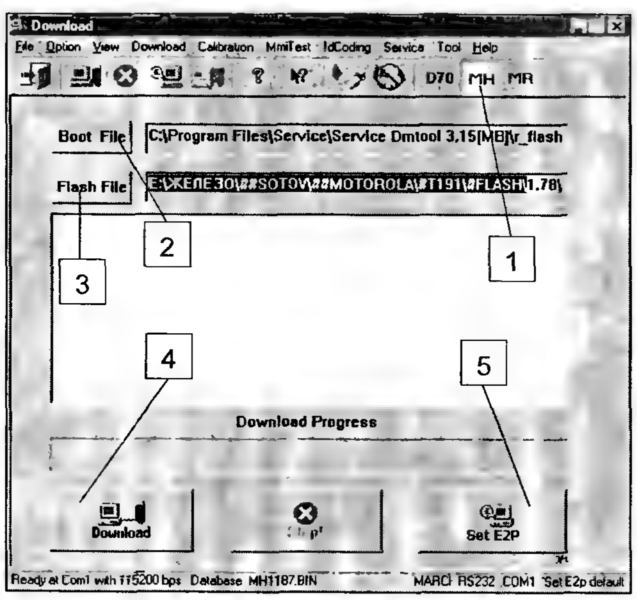


Рис 5 8

Рис 5 9

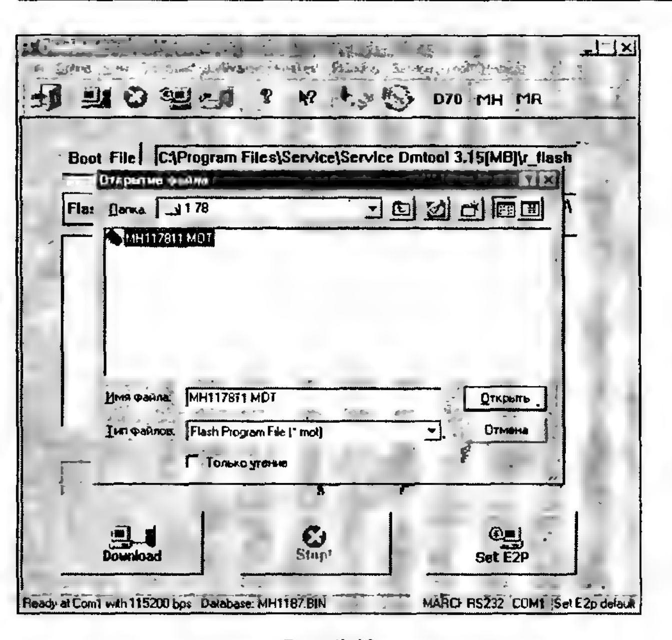


Рис. 5.10

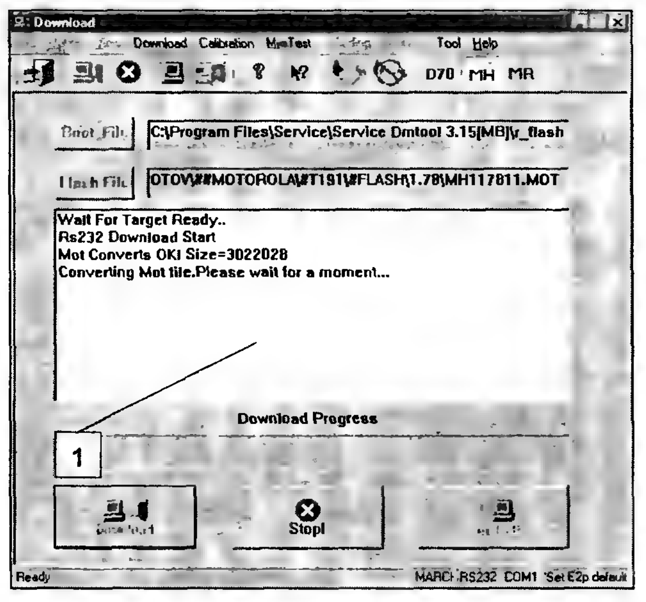


Рис. 5.11

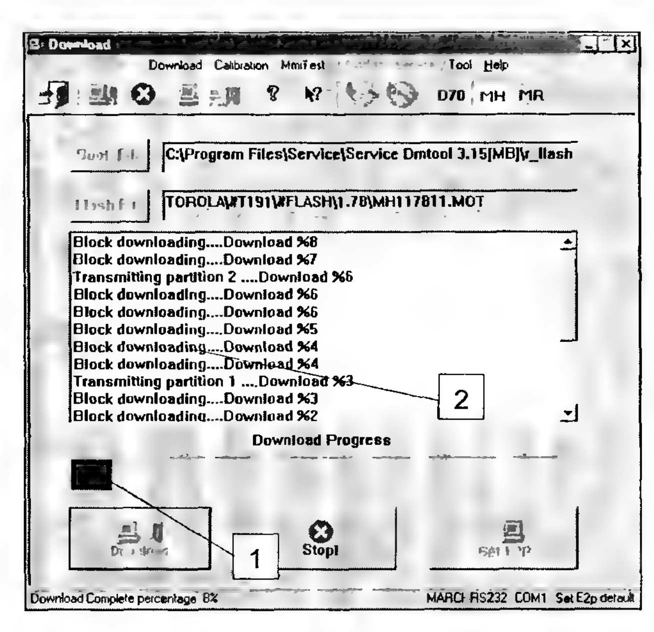


Рис. 5.12

Рис. 5.13

(рис. 5.12). Аналогичный индикатор появится и на дисплее телефона (рис. 5.13). В окне 2 на ПК будет отображаться информация о ходе выполнения копирования. По окончании процесса записи окно программы будет иметь вид, показанный на рис. 5.14, а из телефона будет слышен короткий двойной звуковой сигнал.

Затем нажимают кнопку (SET E2P 5 рис. 5.8) — и, кратковременно, кнопку включения питания на телефоне — для того, чтобы произвести установку заводских настроек на аппарате (о чем говорилось выше). По окончании процесса начального сброса из телефона раздастся двойной короткий звуковой сигнал.

Затем можно включить телефон и проверить его работоспособность в различных режимах.

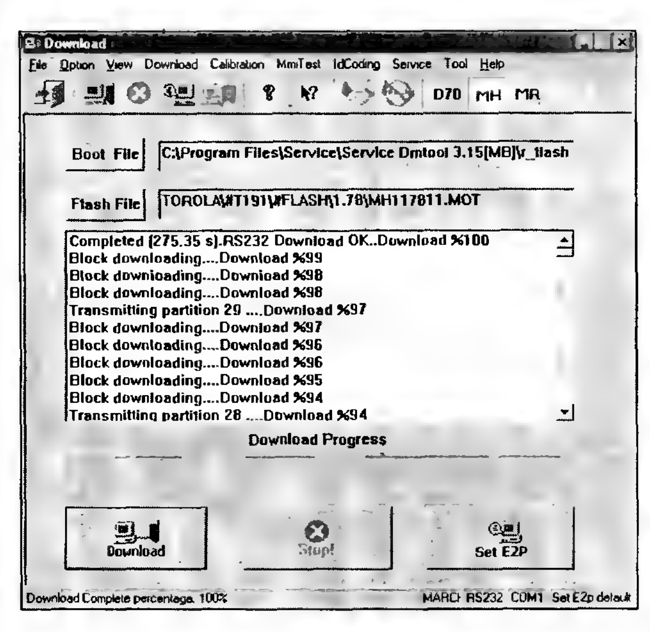


Рис. 5.14

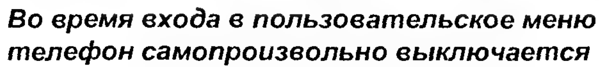


Рис. 5.15

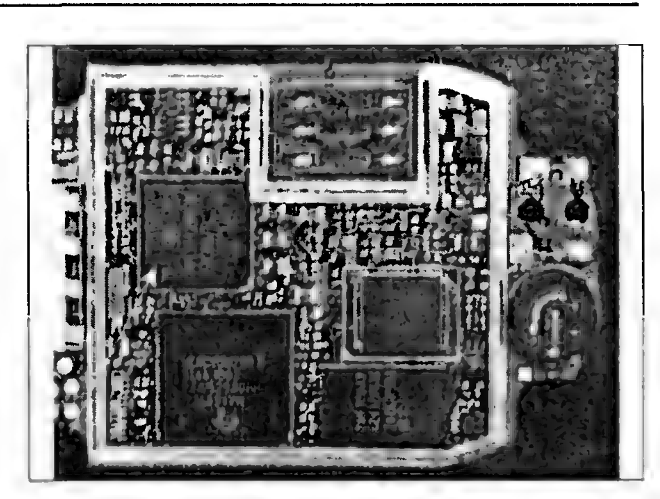


Рис. 5.16

Рис. 5.17

Во время входа в пользовательское меню телефон самопроизвольно выключается

Сначала рекомендуется сделать сброс EEPROM на заводские установки. Если это не помогло, то определяют версию ПО, набрав на клавиатуре следующую комбинацию: *#300# и затем — зеленую кнопку ОК (показана стрелкой на рис. 5.2).

Узнав версию ПО, записывают его заново по методике, описанной в предыдущем пункте.

На экране телефона отображается сообщение «ILLEGAL SOFTWARE LOADED»

Внешний вид сообщения на экране телефона показан на рис. 5.15. Подобное сообщение появляется в двух случаях.

Первый случай связан с производственным браком партии телефонов, выпущенных в мае 2002 г. Это связано с проблемой совместного использования микросхемы аудиоконтроллера типа OMEGA (TWL3011xxx или TWL3012xxx) и конденсатора С16. В бракованной партии на стикере под аккумуляторной батареей в строке MSN содержится буква «С» (5-е знакоместо) или «J» и «K» (6-е знакоместо). Расположение микросхемы аудиоконтроллера на плате телефона показано стрелкой на рис. 5.16. Для устранения подобного дефекта удаляют конденсатор С16, расположенный рядом с соединителем SIM-карты (рис. 5.17).

В партиях аппаратов с микросхемой OMEGA, выпущенных после 22 мая 2002 г., конденсатор С16 уже не устанавливается.

Второй случай связан с некорректной загрузкой ПО во флэш-память телефона. Например, если на стикере металлического экрана телефона (см рис. 5.6) написано MH117611 (что соответствует версии ПО 1.76), а в телефоне установлена версия 1.87 (MH118711) или, что хуже, наоборот. При попытке записи программой DMTOOL «родной» версии ПО, отображается сообщение об ошибке. Выходом из подобной ситуации может быть загрузка так называемой «пропатченной» версии ПО (см. ниже). После загрузки нового ПО обязательно выполняют начальный сброс телефона до заводских устанавливают (нажав кнопку SET E2P) и затем заново устанавливают «заводское» ПО.

Телефон нормально работает во всех режимах, но при этом постоянно звонит (зуммер включается даже в выключенном телефоне в момент зарядки АКБ)

Еще этот дефект называют TAMPER ALERT. Подобная ситуация возникает, если произошел какой-то серьезный сбой в ПО телефона, вызванный, например, неправильной разблокировкой.

Причина дефекта — разрушение данных (или сбой) в области EEPROM микросхемы FLASH-памяти.

Примечание. *Во многих телефонах используется микросхема электрически стираемого перепрограммируемого постоянного запоминающего устройства (ЭСППЗУ) Многим известна распространенная серия этих микросхем — 24Cxx В микросхемах, установленных в телефоны, хранятся пользовательские и иные данные о настройках аппарата В аппаратах «Motorola T190/191» микросхемы EEPROM физически отсутствуют (как и в большинстве других телефонов), под нее выделяется область в микросхеме FLASH-памяти.*

Рис. 5.18

Существует два наиболее распространенных (и безопасных) способа, с помощью которых можно устранить подобный дефект. Рассмотрим их более подробно.

Вначале необходимо определить тип FLASH-памяти, установленной в аппарат В указанных телефонах наиболее часто используются микросхемы FLASH от INTEL. 28F320C3T (серия «С») и 28F320J3 (серия «J»).

Способ 1

Для восстановления области EEPROM в микросхемах FLASH-памяти С-серии используют программу «Motorola T19x Service Software», еще ее называют «ХАК» (рис. 5.18). С помощью этой программы также можно снимать блокировки телефона, активировать дополнительные языки в меню аппарата и изменять IMEI-номер.

Назначение некоторых ее элементов следующее:

— окно 2 служит для выбора режимов Unlock (включить режим разблокировки), Activate Languages (активировать дополнительные языки меню) и Change IMEI (смена IMEI-номера);
— окно 3 служит для ввода нового IMEI-номера;
— окно 4 Write Log File служит для разрешения записи в файл последовательности выполняемых операций в окне 6;
— окно 5 Auto Loop выбирает автоматический цикл при выполнении той или иной операции;
— индикатор 7 служит для отображения выполнения операции или для копирования;
— кнопка 8 Do It — то же, что ОК (при выполнении операций в окнах 2 и 3);
— кнопка 9 Abort — отмена выполнения операции;
— кнопка 10 Tamper Alert Repair — запуск операции восстановления телефона.

Примечание. Указанную программу нельзя использовать с микросхемами FLASH-памяти серии J

Порядок работы с программой следующий:

— в окне «Port» выбирают номер СОМ-порта (1 на рис. 5.18) ПК, к которому будет подключен DATA-кабель;
— снимают все флажки в окнах 2 и 5, устанавливают флажок в окне 4;
— подключают выключенный телефон через DATA-кабель к ПК;
— нажимают кнопку 10 (Tamper Alert Repair);
— нажимают кнопку включения питания на телефоне;
— на индикаторе 7 появится шкала, которая достигнет значения 6...7%. Затем в окне 6 появится сообщение, требующее включения телефона. После этого еще раз нажимают кнопку включения;
— через некоторое время шкала на индикаторе 7 достигнет значения 100%, в окне появится сообщение о завершении операции и после этого из телефона будет слышен двойной звуковой сигнал.

Отсоединяют телефон от DATA-кабеля, включают его и проверяют во всех режимах работы.

Способ 2

Для восстановления области EEPROM в микросхемах FLASH-памяти серии J используют программу SERVICE DMTOOL (рис 5.8). Для этого необходим специальный «пропатченный» или как его по другому называют — «ремонтный» файл Например, для версии ПО 1 70 файл может иметь вид: MH117011_SAVE.MOT (или для версии 1.89 — MH118911_SAVE.MOT).

В отличие от «заводских», в этих файлах определенным образом модифицированы области

флэш-памяти, вследствие чего восстанавливается областьEEPROM после записи в телефон.

Эти файлы загружают обычным способом. После загрузки необходимо выполнить начальный сброс телефона до заводских установок (нажав кнопку SET E2P программы DMTOOL).

Но это еще не все. После загрузки «пропатченного» файла устанавливают «заводское» ПО, например, версий 7.73 (MH177312.MOT) или 7.81. Отметим, что если была прошита версия «лечебного» файла 1.89 (MH118911_SAVE.MOT), то «заводское» ПО должно иметь версию 7.81. После загрузки ПО выполняют начальный сброс телефона до заводских установок.

Информация для любознательных

Бывают ситуации, когда в силу определенных факторов (по неопытности ремонтника и др.), в телефоне стирается BOOT-область (область загрузчика) FLASH-памяти. Аппарат в этом случае не только не включается, но и отсутствует связь с ПК через DATA-кабель.

Для восстановления BOOT-области можно воспользоваться стандартным программатором микросхем FLASH-памяти (выполнить копию прошивки FLASH-памяти с любого исправного аппарата). Для этого выпаивают микросхему флэш-памяти с исправного аппарата, считывают ее содержимое на программаторе и затем прошивают на нем микросхему с неисправного телефона.

Кроме того, в качестве программатора можно использовать любой телефон, в котором стоит аналогичная FLASH-память, и в котором BOOT-область записана в память процессора (например, «Siemens C45» или «Nokia 3330/6210»). Остановимся на втором варианте более подробно.

Следует отметить, что если в аппарате установлена FLASH-память серии J, ее лучше сразу заменить микросхемой серии C (в микросхемах серии J область BOOT таким способом восстановлению не подлежит).

Для восстановления BOOT-области необходимо следующее оборудование:

— аппарат «Motorola T190/191» с неисправной FLASH-памятью типа C (в котором необходимо восстановить область загрузчика во FLASH-памяти);
— исправный аналогичный аппарат «Motorola» (с памятью типа C);
— один из аппаратов «Siemens C45» (или «Nokia 3330/6210») — для программирования FLASH-памяти типа F320C3x от «Motorola T191» или «Nokia 3210/3310» — для памяти F160C3TC от «Motorola T190».

В перечисленных аппаратах-программаторах должна быть исправна процессорная часть (они должны связываться с ПК). Кроме того, для них необходимы соответствующие DATA-кабель и ПО;
— паяльная станция.

Последовательность операций по восстановлению BOOT-области в неисправном аппарате «Motorola» следующая:

— с помощью паяльной станции выпаивают микросхему FLASH-памяти из рабочего аппарата «Motorola»;
— впаивают указанную микросхему в любой из перечисленных выше аппаратов-программаторов «Siemens» или «Nokia» (предварительно из него выпаивают «родную» микросхему FLASH);
— с помощью ПК (под управлением ПО через соответствующий DATA-кабель) считывают и сохраняют все содержимое FLASH-памяти. Размер считанного файла для аппаратов «Motorola T191» с FLASH-памятью F320C3x — 4096 Кбайт, а для моделей T190 с памятью F160C3TC — 2048 Кбайт; в формате *.bin или *.fls.
— выпаивают рабочую микросхему FLASH-памяти из аппарата-программатора и впаивают микросхему с поврежденной BOOT-областью;
— записывают предварительно считанный файл в эту микросхему;
— устанавливают прошитую микросхему в ранее неисправный аппарат, телефон должен включиться, после чего выполняют начальный сброс (SET E2P).

Примечание. *Можно предварительно считать данные с FLASH-памяти с запорченным содержимым и сравнить полученный файл с файлом, считанным с исправной микросхемы, в любом HEX-редакторе. Увиденные различия помогут разобраться в организации памяти телефона и наглядно увидеть повреждённые данные. Если вы будете знать, как восстановить поврежденные данные, то сможете это делать сразу в программаторе, не перезаписывая FLASH-память целиком.*

Описанная выше методика, на первый взгляд, является сложной для повторения, так как требует выполнения большого количества операций пайки. Однако, основное ее достоинство в том, что для восстановления FLASH-памяти не требуется приобретение дорогостоящего программатора.

Глава 6. Сотовые телефоны MOTOROLA

Модель: «Motorola E365»

Телефон «Motorola E365» в настоящее время является одной из самых доступных и популярных моделей на российском рынке. Аппарат выполнен на платформе COMPAL и, по своим схемотехническим решениям, а также особенностям программирования, мало чем отличается от модели «Panasonic G60». Программное обеспечением для работы с этой моделью очень похоже на ПО DMTOOL для телефонов MOTOROLA на платформе ACER — T205, T190 и T191 (см. главу 5), а пользовательский интерфейс такой же, как у PANASONIC G60 SERVIVE TOOL. DATA-кабель для 365-й модели почти полностью подходит от «Motorola T205», только в нем необходимо переставить перемычку на системном соединителе с конт. 6—10 на 1—6. Также в качестве основы можно использовать кабель, например, от телефонов «Motorola T190/T191». Нужно только незначительно изменить его схему и заменить системный соединитель. Аналогичный соединитель используется в телефонах «Motorola STAR TAC» — «Motorola V50», а также «Motorola TIMEPORT» и «Benefon Q». Принципиальная схема одного из вариантов DATA-кабеля для телефона «Motorola E365» приведена на рис. 6.1. Рассмотрим особенности программирования этой модели.

Установка управляющей программы на ПК

Смена версии ПО (при увеличении порядкового номера версии) необходима с целью более устойчивой работы телефона, а также для расширения его возможностей. Оригинальное (заводское) ПО на ПК для прошивки этого типа телефона называется E365 SERVICE TOOL. Рекомендуется установить на ПК две версии этой программы — 1.7 и 2.0. Для этого сначала устанавливают программу E365 SERVICE TOOL ver. 1.7 (C:\Program Files\E365 SERVICE TOOL). Затем копируют файл **st1.7.exe** из этой папки в любое другое место дискового пространства ПК, после чего удаляют программу E365 SERVICE TOOL (стандартными средствами Windows — через «Установку и удаление программ» в «Панели управления»). Устанавливают версию 2.0 этой программы и в ее папку снова копируют загрузочный файл версии 1.7, предварительно переименовав его, чтобы ОС не предложила перезаписать файл в этой директории из-за совпадения имен. Таким образом, в папке E365 SERVICE TOOL будут находятся одновременно два загрузочных файла для разных версий. Дело в том, что эти версии взаимно дополняют друг друга: в версии 1.7 активированы одни режимы работы, а в версии 2.0 — другие. Указанные ограничения присущи только так называемым бесплатным версиям этой программы (которые находятся в свободном доступе, например, в Интернете).

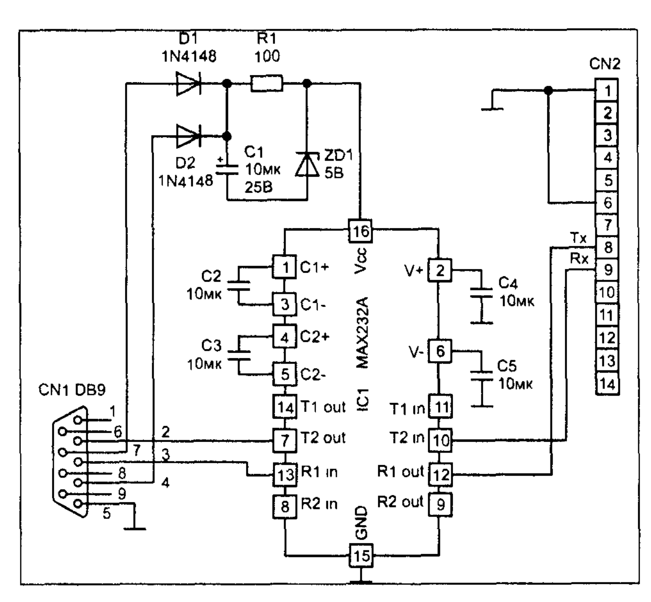


Рис. 6.1

Настройка ПО на ПК

После запуска программы SERVICE TOOL (например, версии 2 0) на экране ПК появится ее основное окно (рис 6.2). Затем в окне программы выбирают модель телефона и ее частотный диапазон: MODEL—E365—900/1800 (рис 6 3)

Затем в окне программы нажимают кнопку OPTIONS — появится окно для ввода пароля (рис. 6.4). В нем набирают пароль (с соблюдением написания строчных и прописных букв) **Compal_T66** и нажимают кнопку ОК.

После этого на экране ПК появится окно, показанное на рис 6.5 В закладке «Connection Setup» выбирают номер СОМ-порта ПК, к которому подключен DATA-кабель, а в закладке «RF Configure» (настройка радиоканала — см. рис. 6.6) — параметры для GSM-тестера (но в нашем случае

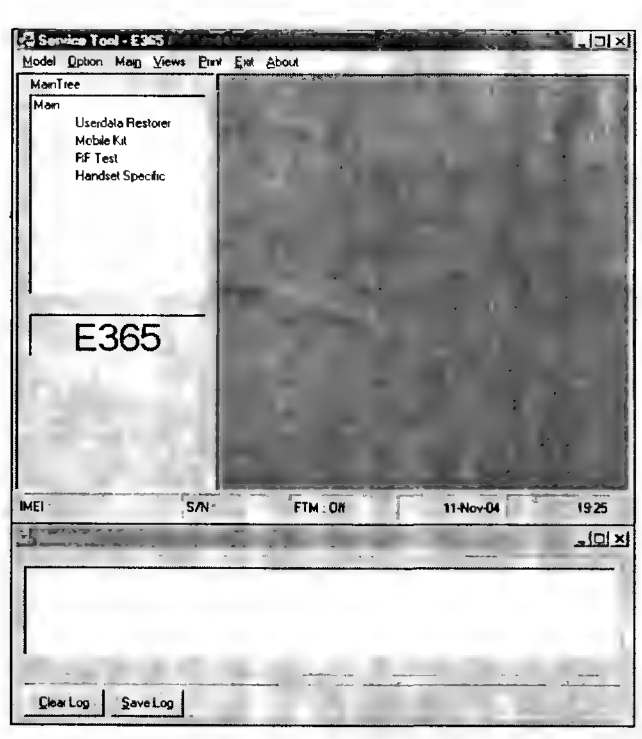


Рис. 6.2

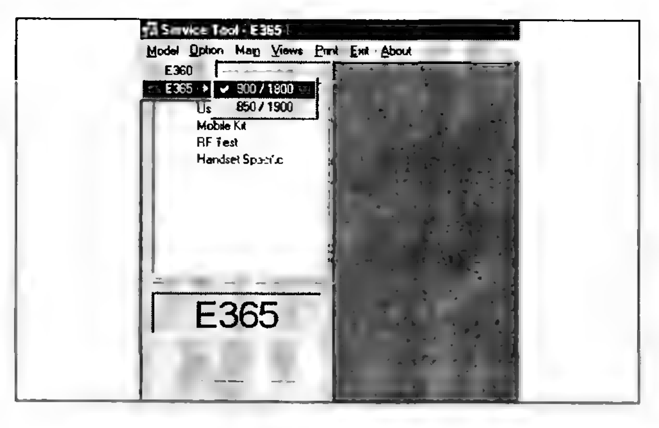


Рис. 6.3

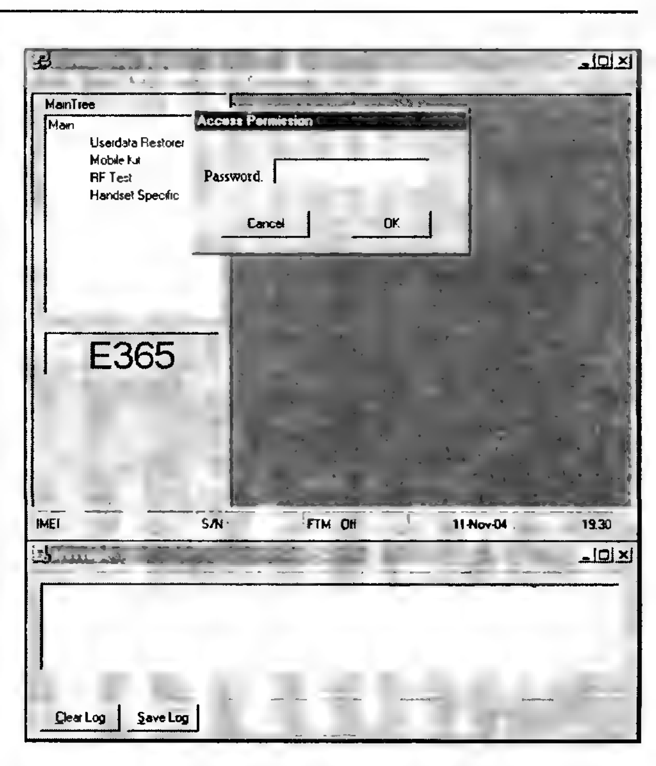


Рис. 6.4

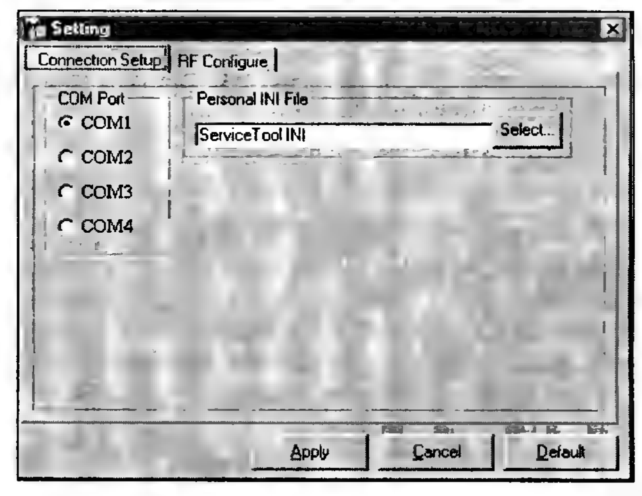


Рис. 6.5

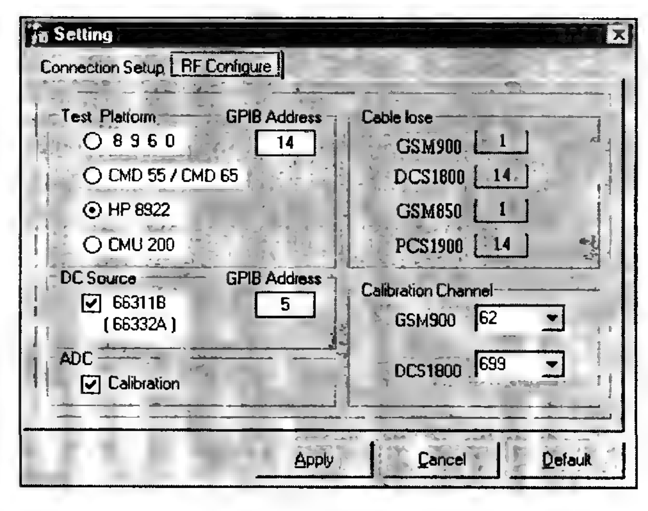


Рис. 6.6

этот прибор не используется). После этого нажимают кнопку Apply (ПРИМЕНИТЬ). Теперь программа готова к использованию. Рассмотрим ее возможности более подробно

Директория «Userdata Restorer»

Для считывания пользовательских данных из аппарата или для их защиты в окне 1 на рис. 6.7 выбирают директорию «Userdata Restorer». Справа появится окно 2, с помощью которого можно сохранить предварительно прочитав, пользовательские данные на жестком диске ПК с телефона. Эту операцию рекомендуется выполнять, если необходимо вернуть пользовательские данные после программирования телефона. Галочки 3 на рисунке указывают, с какой частью пользовательских данных будут гроводиться операции чтения и сохранения на диск ПК: Phonebook — телефонная книга, OICQ — интернет-пейджер, QuickNotes — блокнот и напоминание, User Data — различные мелодии, картинки и другие пользовательские файлы.

Далее необходимо подключить телефон (во включенном состоянии) к ПК через DATA-кабель и нажать в окне программы кнопки Read Data — для чтения данных из телефона) или Write Data — для записи данных.

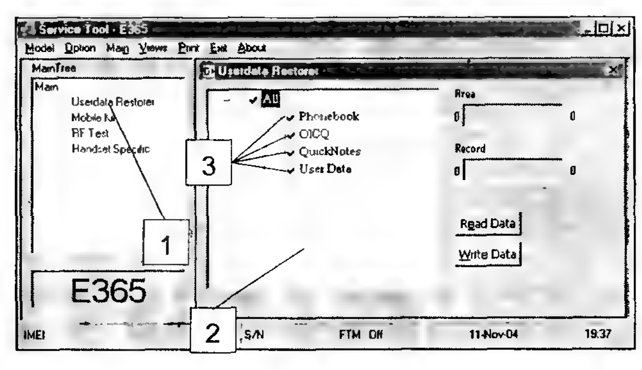


Рис. 6.7

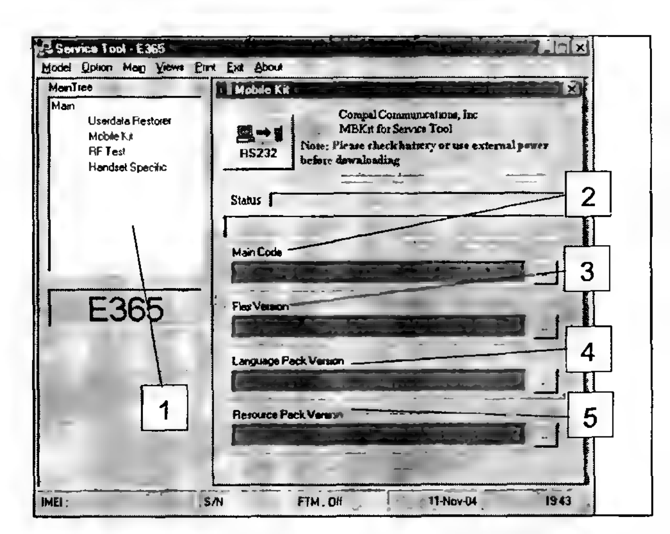


Рис. 6.8

Директория «Mobile Kit»

Для перепрограммирования ПО телефона в окне 1 (рис. 6.7 и 6.8) выбирают директорию «Mobile Kit», справа появится окно с соответствующим именем (рис. 6.8). Вид окна, показанный на рисунке, соответствует версии 2.0 программы E365 SERVICE TOOL. В версии программы 1.7 окно выглядит по-другому (рис. 6.17), его возможности ограничены, поэтому мы будем рассматривать работу с этим окном на примере версии 2.0. В этом окне указывается местонахождение файлов на диске ПК, необходимых для программирования телефона.

В этом окне в директории «Main Code» (2 на рис. 6.8) выбирают основной flash-файл прошивки (рис. 6.9) ПО телефона — его еще называют ядром ПО. Файл может иметь следующее название: **T66E.0.1.48.mot**, и его размер приблизительно равен 20 Мбайт.

Затем в директории «Flex Version» (3 на рис. 6.8) выбирают файл области памяти телефона, хранящей различные настройки, например, опции и пункты меню аппарата. Файл может иметь название: **Flex.T66.63.50.09RSPK.T66.63.50.01.mot**.

В директории «Language Pack Version» (4 на рис. 6.8) выбирают файл языкового пакета (например, **LP.T66E.0.1.29.1.mot** — см. рис. 6.9), а в

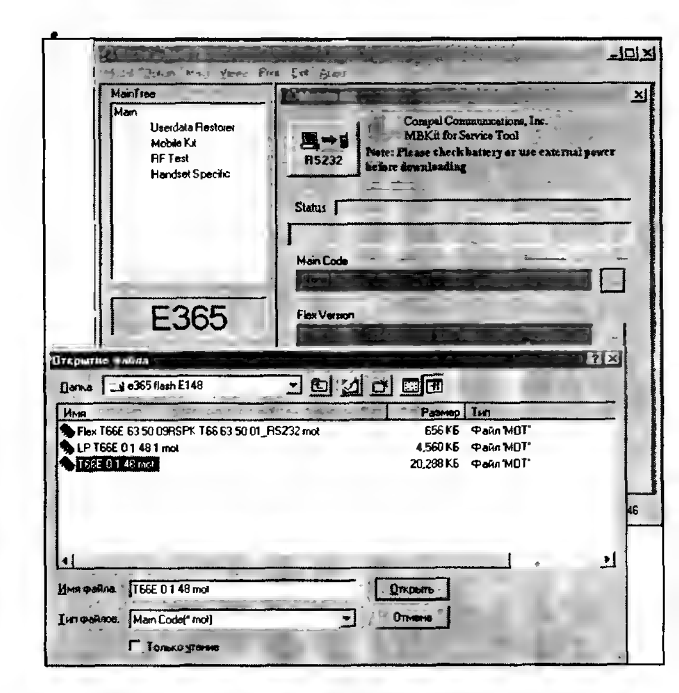


Рис. 6.9

«Resource Pack Version» (5 на рис. 6.8) — файл ресурсов **RSPK.T66.63.50.01.mot**. (рис. 6.10).

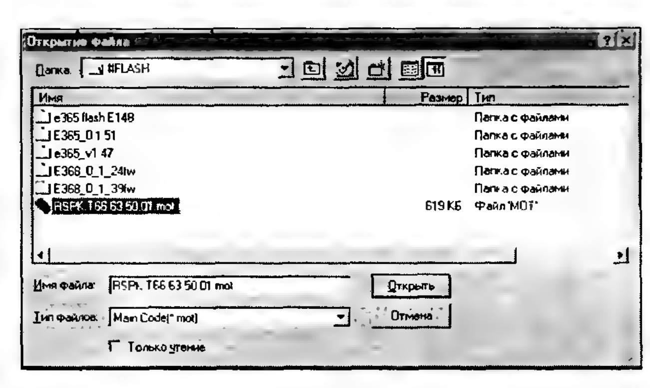


Рис. 6.10

Следует отметить соответствие файлов языковых пакетов Language Pack тому или иному региону

— **LP.T66E.0.1.29.1.mot** — страны СНГ и Балтии, а также Западной и Восточной Европы,
— **LP.T66E.0.1.29.2.mot** — Китай,
— **LP.T66E.0.1.29.3. mot** — страны Африки

После выбора файлов окно программы примет вид, показанный на рис. 6 11.

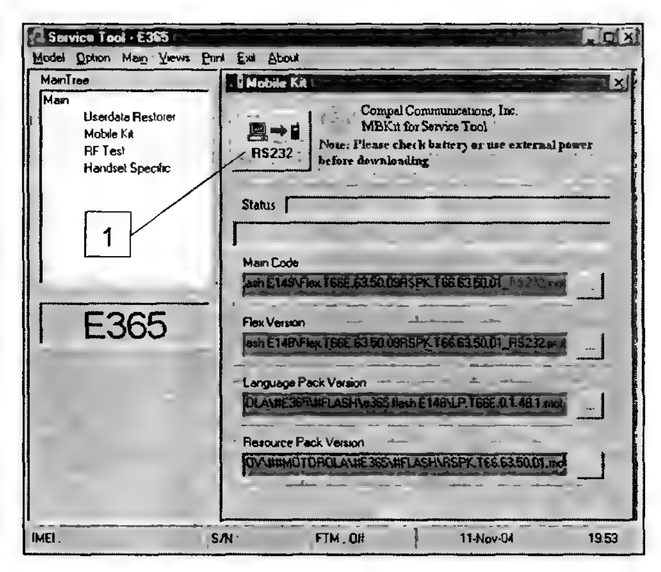


Рис 6.11

Следует заметить, что если необходимо перепрограммировать только FLEX или MAIN, достаточно указать путь только к одному из этих файлов.

Прошивка ПО телефона и другие возможности программы E365 SERVICE TOOL

После настройки программы E365 SERVICE TOOL присоединяют выключенный телефон (без SIM-карты) к DATA-кабелю, нажимают кнопки 1, в появившемся окне — OK и, кратковременно, кнопку включения самого телефона (рис 6.11).

После этого будет выполняться операция записи ПО во FLASH-память телефона, в процессе которой появится индикатор копирования 1 (рис 6.12), а в окне 2 «Message» — информация о ходе копирования По окончании копирования на экране телефона высветится сообщение «SW Initialise!!» (рис 6 13), а затем произойдет автоматическое включение аппарата и появится сообщение «Вставьте SIM» (рис 6 14). После этого выключают телефон, вставляют в него SIM-карту, включают аппарат и проверяют его работоспособность

Сам процесс копирования занимает около 15 минут (если переписываются все четыре вида

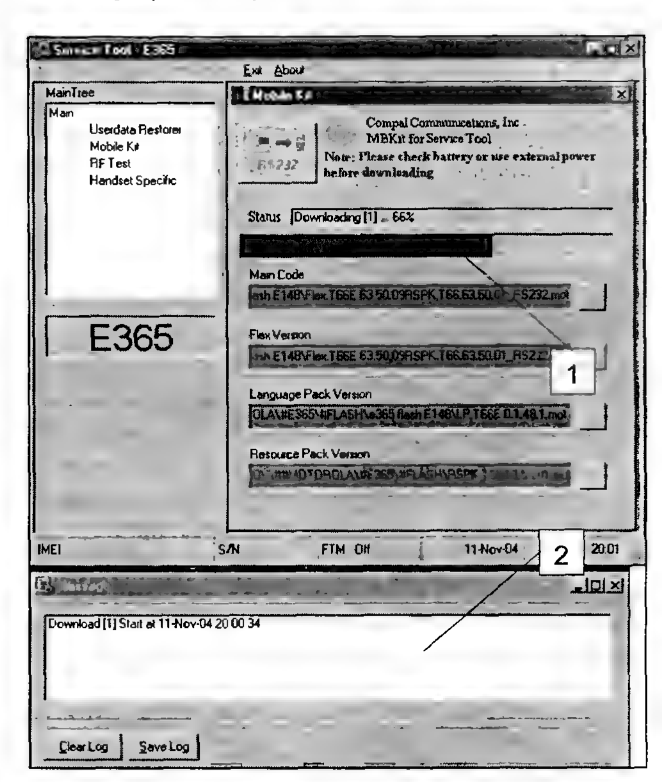


Рис. 6.12

Рис. 6.13

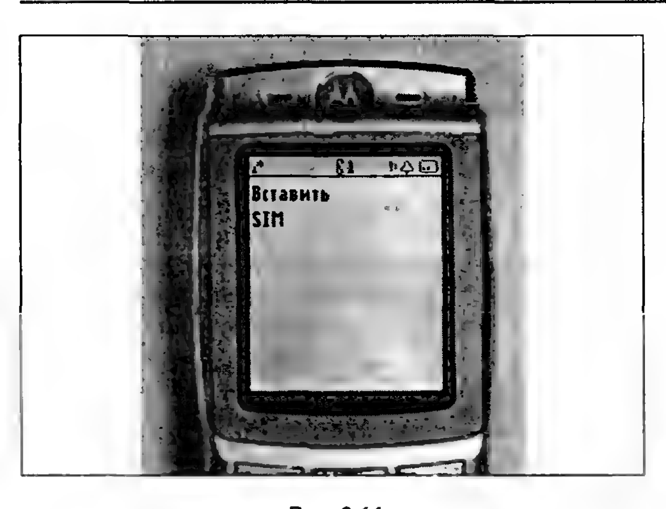


Рис. 6.14

файлов — Main Code, Flex Version, Language Pack Version и Resource Pack Version).

При замене версий ПО телефона следует учесть, что можно записать только аналогичную или позднюю версию.

Директория «Handset Specific»

Для получения справочной информации о телефоне вернемся к основному окну программы E365 SERVICE TOOL — в нем выбирают директорию «Handset Specific» (рис. 6.15), включают телефон (без SIM-карты), подключают к нему DATA-кабель и в окне программы нажимают кнопку 1 Read Data. В пустых графах правого окна программы появится информация о его IMEI-номере, версии языкового пакета и др. (рис. 6.16). Перечислим еще некоторые позиции этого окна:

SW Version — версия ПО телефона;
Flex Version — версия Flex-файла;
TFT — счетчик наработки.

Кнопкой 1 (рис. 6.16) Power Cucle проводят перезагрузку аппарата.

На этом рисунке также показана кнопка 2 — EFEM (ON/OFF), которая разрешает или запрещает включение режима тестового меню телефона (сообщение 4 «FTM. ON» внизу окна говорит о том, что тестовое меню включено).

Это меню позволяет·

- выполнить с клавиатуры телефона различные настройки;
- тестировать аппаратную и программные части телефона;
- произвести общий сброс телефона и т. д.

В этой статье тестовое меню рассматриваться не будет. Более подробную информацию об активации меню и порядке работы в нем можно найти в сервисной документации на указанный тип телефона (уровень 2 и выше).

С помощью директории «Handset Specific» также можно снять код блокировки телефона, нажав в ней кнопку 3 UnLock (рис. 6.16).

Отметим, что кнопки EFEM, UnLock и Power Cycle в версии 2.0 программы E365 SERVICE TOOL, а также UPDATE **не активны!** Они активны только в версии 1.7.

Также отметим, что одним еще одно отличие версии 2.0 от 1.7 этой программы Версия 2.0 позволяет выполнить как выборочное, так и одновременное копирование файлов директорий «Main Code», «Flex Version», «Language Pack Version» и «Resource Pack Version». С помощью версии 1.7 возможно только выборочное копирование файлов (только Flex или только Main Code — см. рис. 6.17. Эта версия не позволяет копировать Language Pack (языковой пакет) и Resource Pack (файл ресурсов).

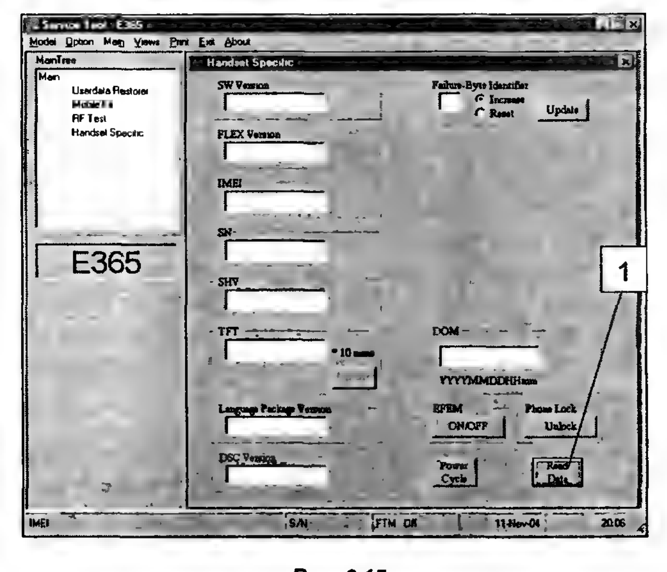


Рис. 6.15

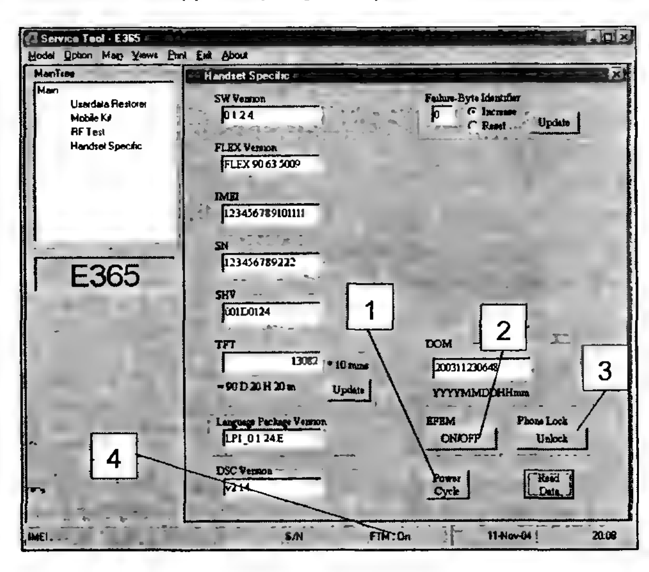


Рис. 6.16

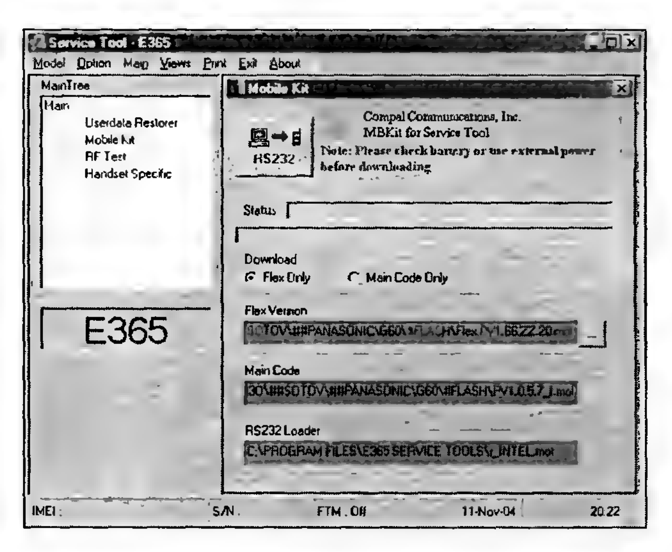


Рис. 6.17

Исходя из сказанного, должно быть понятно, почему при инсталляции программы E365 SERVICE TOOL версии 2.0 дополнительно устанавливают ее более раннюю версию 1.7.

Примечание. *При работе с программой E365 SERVICE TOOL (окно 1 на рис 6 7) необходимо соблюдать определенную последовательность После запуска программы, с целью получения справочной информации о версии ПО телефона, вначале выбирают директорию «Handset Specific» Затем в директории «Userdata Restorer» при необходимости считывают пользовательские данные В заключение, в директории «Mobile Kit» выбирают файлы прошивки и программируют FLASH-память телефона*

Если телефон включается, много справочной информации о нем можно получить, набрав с клавиатуры команду #02#. После этого на экране телефона можно ознакомиться с информацией о версии ПО телефона (рис. 6.18), версии Flex-файла, языкового пакета и другой информацией (рис. 6.19).

Разблокировка телефона

Снятие пользовательской блокировки можно проводить с помощью программы E365 SERVICE TOOL (рис 6 15, кнопка 1 UnLock). Для снятия операторских блокировок существует другие программы. Остановимся на двух из них.

Первая программа — E365 NSK READER, ее окно в момент чтения операторских кодов разблокировки показано на рис. 6.20. По окончании этого процесса в окне 1 (рис. 6.21) отобразятся коды — их набирают на клавиатуре телефона.

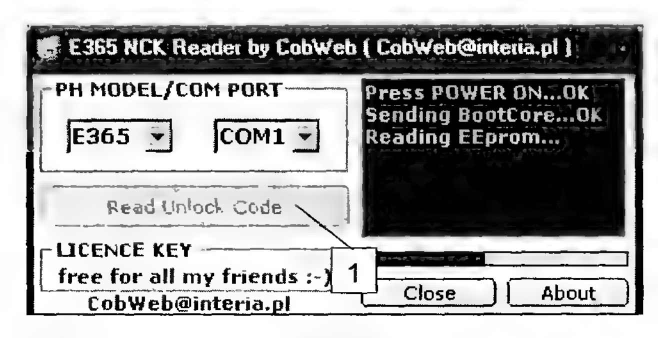


Рис. 6.20

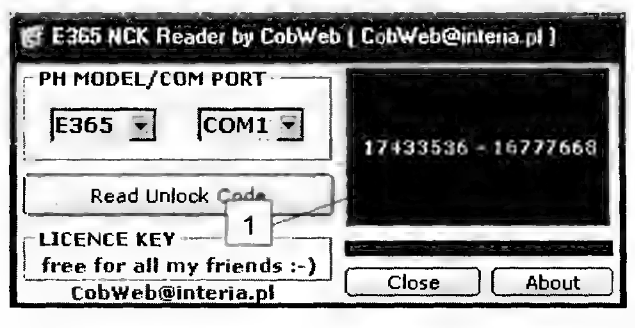


Рис. 6.21

Отметим, что после загрузки программы нажимают кнопку 1 «Read Unlock Code» (рис. 6.20), а затем, кратковременно, кнопку включения телефона.

Вторая программа — MOT TOOL C200/E365/T190/T191, ее основное меню показано на рис. 6.22. Она позволяет проводить не только разблокировку/блокировку телефона, но и чтение/запись данных flash-памяти (как выборочно, так и полностью), установку пользовательского кода на заводской и другие операции. Пользовательский интерфейс программы достаточно понятен, поэтому подробно останавливаться на ней мы не будем.

Кроме того, есть еще одна оригинальная (заводская) программа — E365_DMTOOL V2.2.02.1, которая кроме разблокировки, позволяет копировать Flex-файл в память телефона. Ее окно показано на рис. 6.23.

Примечание. 1 Все управляющие программы для этой модели телефона (например, E365 NSK READER и др) «реагируют» на кратковременное нажатие кнопки включения аппарата спустя 3 с
2 Чтобы снять пользовательскую (или операторскую) блокировку аппарата, достаточно записать во FLASH-память телефона

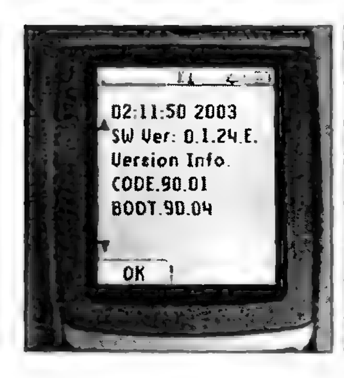


Рис. 6.18

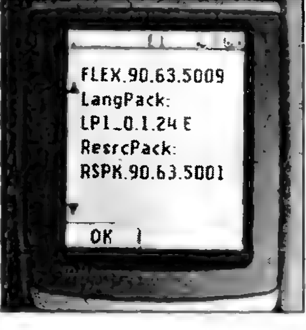


Рис. 6.19

*Flex файл называемый **unlock_E365 mot** Это можно выполнить как с помощью программы E365_DMTOOL так и других например, E365 SERVICE TOOL*

Программный ремонт телефона

Телефон не включается

С помощью любой из приведенных выше программ, переписывают Flex-файл в память телефона (например, **unlock_E365.mot)**

Если процесс записи прошел успешно, запускают E365 SERVICE TOOL версии 2 0 и с помощью нее записывают файлы Main, Flex и Language Pack (Resource Pack записывать не нужно)

При переполнении пользовательской памяти телефона (например, большим количеством фотоснимков), в момент его включения, он «зависает» на логотипе «HELLOMOTO» (см. рис. 4.24)

Быстрый способ устранения подобной проблемы (но не самый надежный) — с помощью перечисленных выше программ переписать Flex-файл в память телефона (**unlock_E365.mot**) После переписи этого файла происходит инициализация ПО аппарата После этого телефон восстанавливает работоспособность, но ненадолго — примерно через неделю подобный дефект может повториться

Чтобы навсегда избавиться от подобной проблемы, с помощью программы E365 SERVICE TOOL в директории Handset Specific считывают данные о версии ПО — Main, Flex, Language Pack

Затем программируют ПО такой же версией или более поздней При этом стирается пользовательская область памяти телефона, которая была переполнена (или содержала ошибки), а также восстанавливаются другие поврежденные области памяти.

Рис. 6.22

Рис. 6 23

Глава 7. Сотовые телефоны MOTOROLA

Телефоны линейки LEGACY

Общие сведения

Все телефоны Motorola линейки LEGACY объединяет один и тот же основной набор микросхем от TEXAS INSTRUMENTS (TI). Перечислим его.

- серия многофункциональных микросхем P79E26/48/58, имеющие в своем составе контроллер питания, аудиоконтроллер и другие компоненты;
- процессоры PD731703/704. Отметим, что в некоторых телефонах используется процессоры от Motorola — SC56683VH3 и 41C42. Эти микросхемы объединяет то, что они имеют одинаковое процессорное ядро (систему команд и основные функциональные узлы).

Кроме того, в этот комплект входят микросхемы оперативной памяти и Flash-памяти.

Перечислим основные типы сотовых телефонов Motorola линейки LEGACY (в скобках даны наименования платформ, на которых они выполнены)

- D-серии — D160, CD160 (MODULUS I), D520 (SPARKY), CD920/930 (ZAP);
- TIME PORT — L7989/7389/7089, P7389 (LEAP), P7689 (JADE);
- M-серии — M3588/3688/3788/3888 (MODULUS II);
- V-серии — V3690/3688/2288/50/51 (KRAMER S3), V100 (CAMELOT);
- T-серии — T180 (ANGEL), T192 (C21), T2288 (SHARK, MODULUS III);
- STAR TAC — 70 (MATRIX), 85 (ALEX), 130 (CRUNCH).

Можно также отметить, что особенности инженерного программирования аппаратов линейки LEGACY в большинстве своем схожи.

Многие телефоны, перечисленные ниже, имеют близкий набор электронных компонентов (аппараты в основном отличаются лишь расположением элементов на печатных платах):

- аппараты D-серии и STAR TAC;
- все аппараты M-серии;
- V-серии (кроме V100);
- некоторые аппараты T и V-серий: T180/2288, V2288;
- некоторые аппараты L и P-серий: L7089, P7089/7389/7689.

Внешний вид аппаратов основных серий линейки LEGACY показан на рис. 7.1

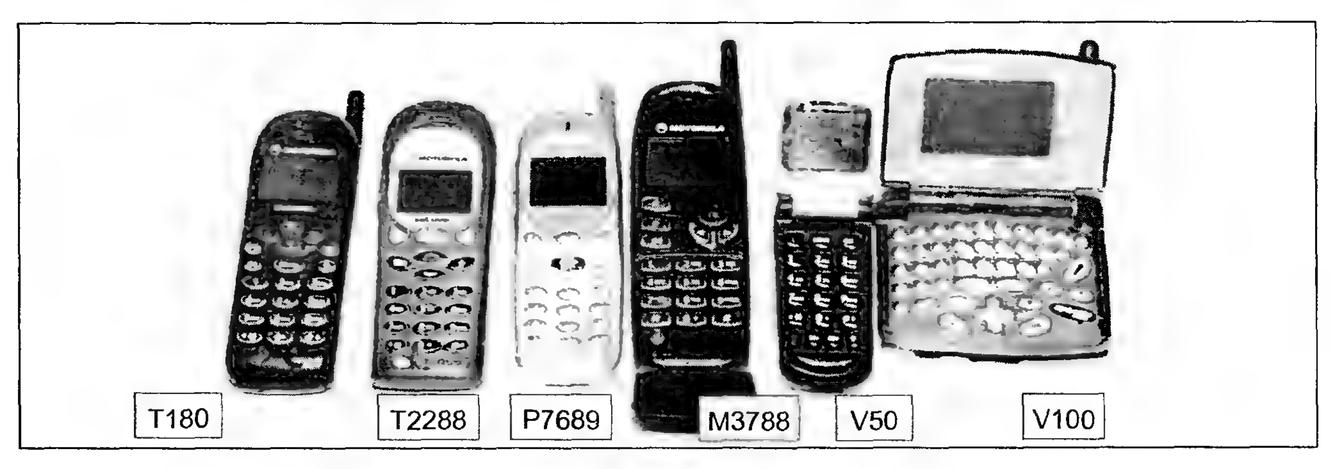


Рис. 7.1

Аппаратные средства для программирования телефонов Motorola линейки LEGACY

В простейшем случае для связи большинства телефонов (с целью их прошивки) и персонального компьютера (ПК) необходим DATA-кабель или универсальный бокс. Для аппаратов Motorola линейки LEGACY все несколько иначе.

Интерфейс EMMI

Начнем с интерфейса, через который происходит программирование этих телефонов — он называется EMMI (ELECTRICAL MAN MASCHINE INTERFACE). Необходимость в разработке этого интерфейса возникла из-за того, что во время создания телефонов LEGACY в ПК использовались всего две распространенных интерфейса для связи с внешними устройствами: последовательный — COM и параллельный — LPT (интерфейса типа USB тогда еще не было). Так как предполагалось иметь высокоскоростной последовательный канал обмена данными между телефоном и ПК, перечисленные выше интерфейсы не удовлетворяли его требованиям. Выходом из подобного положения стало создание специалистами компании Motorola интерфейса EMMI.

EMMI-интерфейс представляет собой подобие последовательного (SERIAL) интерфейса, работающего на более высоких скоростях. Скорость стандартного SERIAL-интерфейса составляет 115200 бит/сек, скорость же EMMI-интерфейса составляет 512000 бит/сек.

Перечислим основные сигналы интерфейса EMMI:

1. GND — общий;
2. DSC ENABLE (или еще встречается аббревиатура DCL) — управление процедурой обработки прерывания (ISR);
3. DOWNLINK — принимаемые телефоном данные;
4. UPLINK — передаваемые телефоном данные.

На рис. 7.2 показано назначение сигналов на внешних соединителях телефонов LEGACY (всего существует 4 типа соединителей), а на рис. 7.3 — внешний вид ответных разъемов для этих соединителей.

Универсальные боксы для программирования телефонов линейки LEGACY

Для программирования с ПК телефонов марки Motorola, использующих EMMI-интерфейс, применяются специальные преобразователи интерфейсов, например, RS232-EMMI (называемый EMMIBOX 2D/3D), а также LPT-EMMI (ROEMMIBOX).

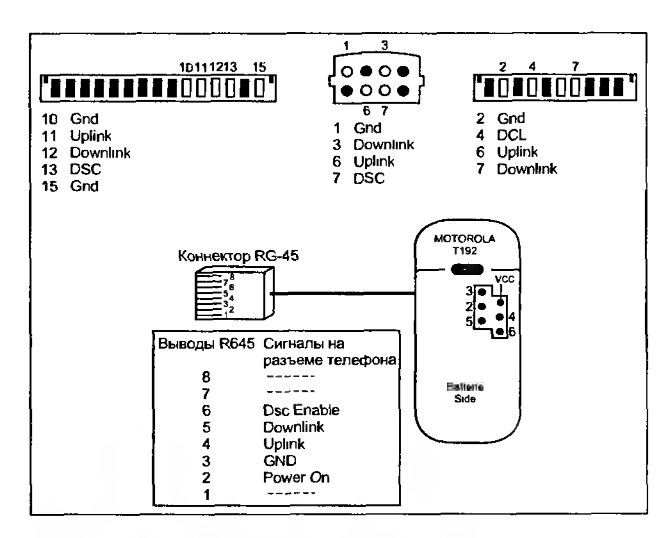


Рис. 7.2

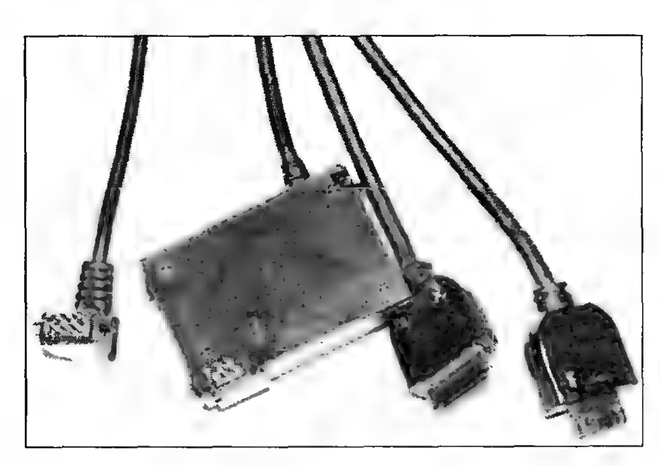


Рис. 7.3

Универсальные боксы EMMI представляют собой достаточно сложные устройства с микропроцессорным управлением. Основная их особенность — они имеют большой объем Flash-памяти, необходимый для хранения программного обеспечения сотового телефона перед его записью в аппарат. Механизм работы ПК с боксами EMMI следующий: вначале в бокс переписывают ПО для конкретного типа телефона (по необходимости — содержимое любой выбранной области Flash-памяти или полный объем ПО — Full Flash), а затем по команде с ПК через EMMI-интерфейс это ПО переписывается уже в сам телефон. Подобный механизм очень удобен, если нужно последовательно «прошить» ПО в большом количестве однотипных телефонов (так как ПО уже находится в буферной памяти бокса, после «прошивки» одного телефона, подключают другой — и так по циклу).

Основное неудобство работы с боксами EMMI (в полной комплектации называемых EMMIBOX 3D) заключается в том, что скорость обмена по

СОМ-порту между ПК и боксом достаточно низкая (115200 бод — запись, 9600 бод — управление), поэтому, например, запись ПО телефона в бокс может длиться 10 15 мин

А уже при обмене информацией между боксом и телефоном (через интерфейс EMMI), скорость обмена значительно выше

На рис 7 4 показан внешний вид одного из вариантов платы EMMIBOX — этот бокс отличается от оригинального только компоновкой и составом ПО бокса (при сохранении всех основных функций) Как видно из рисунка, на плате имеются следующие основные элементы управляющий микроконтроллер типа MC68332, преобразователь интерфейса EMMI (микросхема BIC (Base Interface Chip) типа 43E08), микросхема ЭСППЗУ типа 24C16 (в ней хранятся данные конфигурирования микросхемы BIC), Flash-память объемом 1 Мбайт (в ней хранится управляющая программа бокса), оперативная память объемом 8 или 16 Мбайт (она предназначена для хранения ПО телефона), а также второстепенные элементы (схема питания, буферные формирователи и др)

Примечание *Есть еще одна разновидность микросхемы BIC (кроме 43E08) — это 43E07 Обе эти микросхемы практически идентичны поэтому подробно останавливаться на их различиях мы не будем При возникновении затруднений с приобретением этих микросхем их можно изъять (выпаять) из старых аппаратов Motorola моделей 5200/6200/7200/8200*

Отметим, что самая распространенная версия прошивки EMMIBOX — 625000 Есть еще более новая версия, называемая 625010, которая позволяет работать с 13 и 14 версиями ПО самих телефонов (не путать с версией прошивки бокса), а также поддерживает телефоны, имеющих Flash-память ATMEL (версия 625000 поддерживает только память INTEL)

Примечание *Если с помощью EMMIBOX (с версией 625000) прошивать ПО на телефоны, имеющее 13 или 14 версии в последних при включении начинает постоянно работать звонок а на дисплее отображается сообщение «TAMPER ALERT»*

Текущую версию ПО телефона определяют через тестовое меню аппарата (см ниже) или при его работе с ПК через EMMIBOX

*Отметим также что формат отображения версии ПО аппарата имеет вид **AA BB CC** где*

AA — буквы соответствующие конкретному типу телефона

BB — цифры означающие номер версии ПО телефона

CC — служебный цифровой код

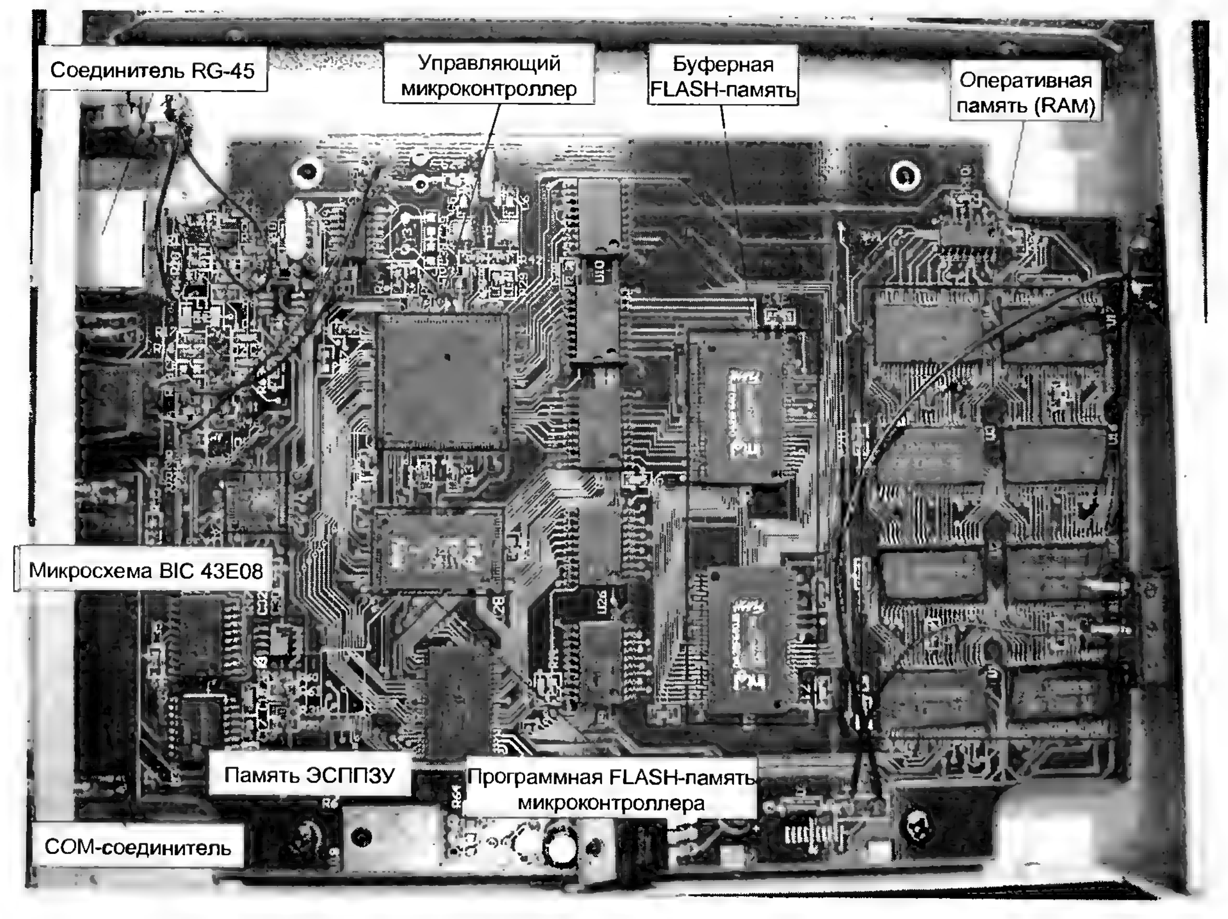


Рис 7 4

Существует множество вариантов боксов EMMI, в том числе есть так называемая модификация ROEMMI. Этот тип бокса еще называют конвертором интерфейсов LPT—EMMI (основное его отличие заключается в подключении бокса к ПК не через COM-порт, а через LPT). Модификаций боксов ROEMMI также большое количество (в том числе и с усеченными функциональными возможностями). На рис. 7.5 и 7.6 приведены принципиальные схемы некоторых из них. Из рисунков видно, что на схемах исключены такие узлы, как оперативная память, управляющий микроконтроллер, Flash-память и др. Скорость обмена этих боксов в цепи: ПК — БОКС — ТЕЛЕФОН одинакова и определяется пропускной способностью LPT-порта (но она ниже максимальной скорости обмена EMMI-интерфейса).

Как запрограммировать FLASH-память EMMIBOX

Начнем с того, что оригинальные EMMIBOX позволяют модифицировать свое ПО с ПК через встроенный COM-порт. Во всех остальных версиях неоригинальных боксов необходимо заново прошивать FLASH-память.

Собственно, EMMIBOX уже поставляются с запрограммированной FLASH-памятью. По различным причинам (разрушение данных FLASH-памяти, желание повысить версию ПО бокса), возникает необходимость заново прошить содержимое микросхемы FLASH-памяти (Intel TE28F800) бокса (см. рис. 7.4).

Так как не у всех ремонтников в наличии имеются программаторы, которые позволяют прошивать FLASH-память, рассмотрим довольно оригинальный способ программирования этого типа памяти с использованием сотового телефона «Ericsson A1018». В этом аппарате уже стоит аналогичный тип микросхемы FLASH-памяти. Кроме телефона необходим DATA-кабель к нему, ПК и управляющая программа для прошивки этого аппарата. Суть программирования микросхемы памяти заключается в том, что вместо файла прошивки для этого телефона выбирается файл для EMMIBOX (для версий 625000 или 625010). Следует отметить, что файлы прошивки как ПО (для Flash), так и содержимое EEPROM (бинарный файл) для EMMIBOX выложены в свободном доступе в Интернете.

После прошивки микросхемы памяти, ее выпаивают из телефона и устанавливают в бокс. Можно, конечно, поступить по-иному: вначале выпаять память из бокса, установить в телефон,

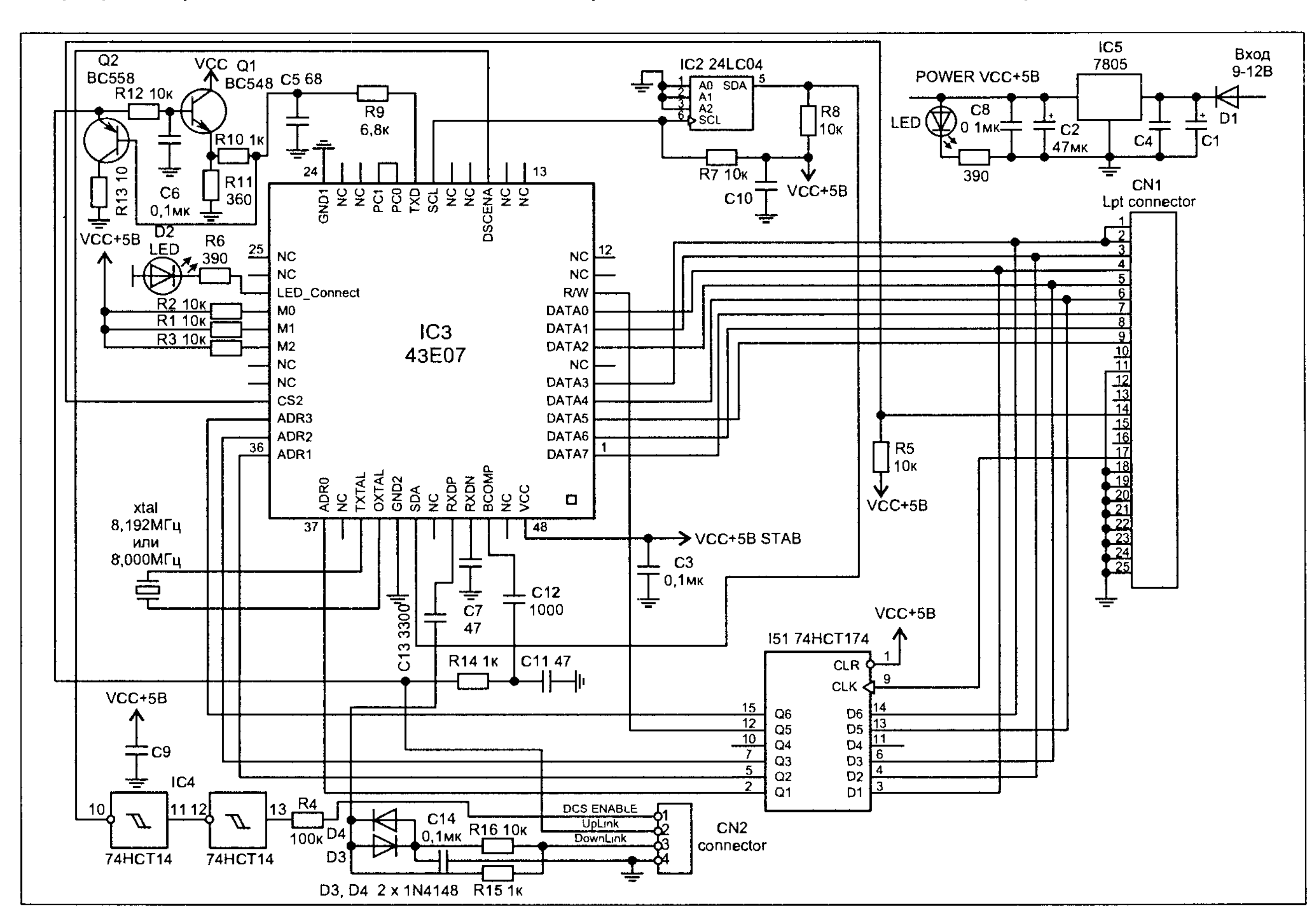


Рис. 7.5

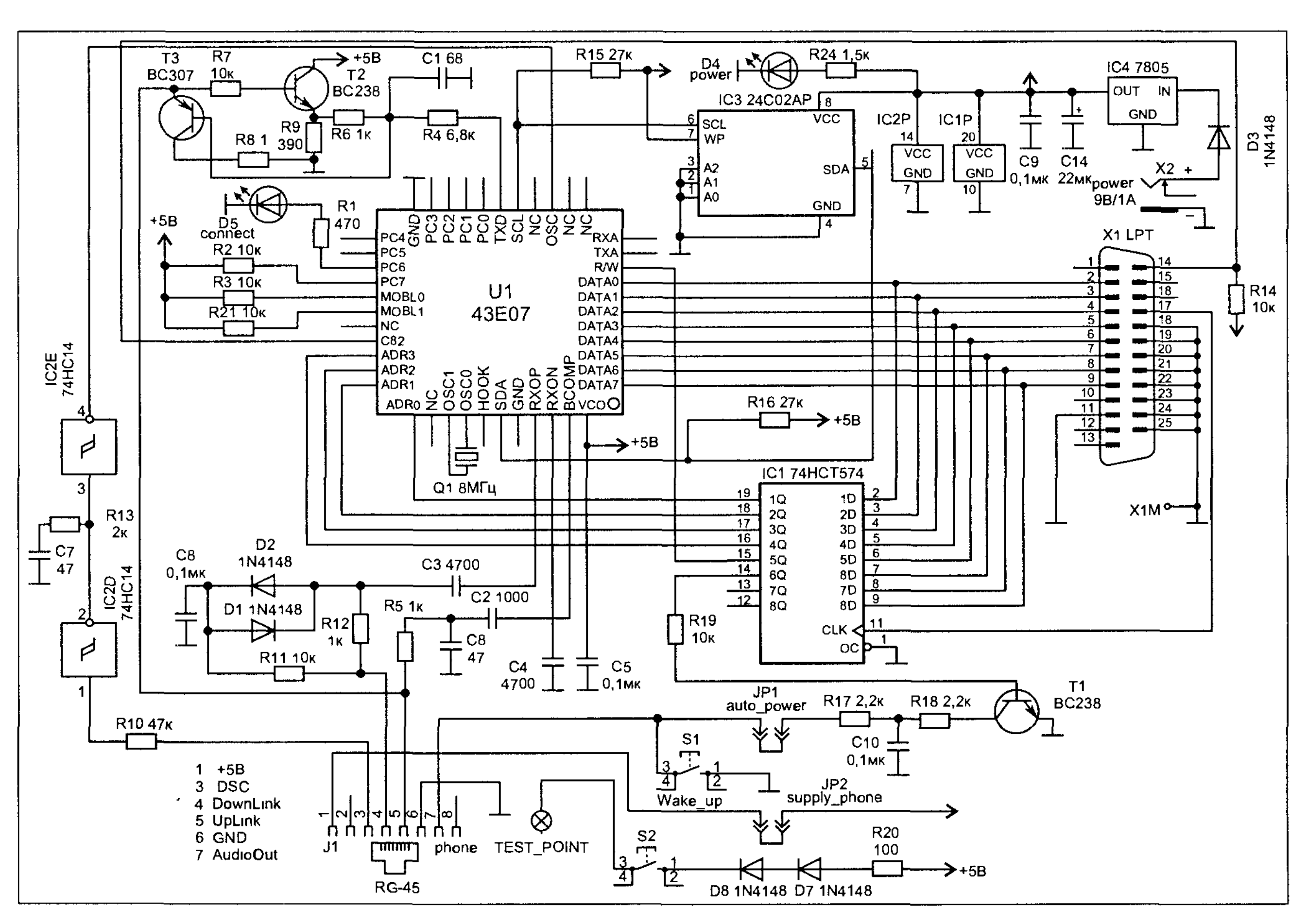


Рис. 7.6

прошить ее, а затем снова установить в бокс — но это не меняет сути процесса.

Аппаратный ключ DONGLE

Существуют универсальные боксы (обычно, производства Юго-Восточной Азии или Китая), которые дополнительно позволяют работать и с телефонами Motorola линейки LEGACY. Для этого в их составе устанавливаются дополнительные аппаратные модули ROEMMI (различных модификаций). Все неудобство работы с ними заключается в том, что для модулей ROEMMI поставляется «сырое» программное обеспечение под оболочку DOS. Для адаптации этих модулей под оболочку Windows, известная по предыдущим публикациям в нашем журнале компания ZULEA предложила собственное программное обеспечение (более подробно мы остановимся на нем в следующих публикациях). Для обеспечения работы ПО от ZULEA, между ПК и боксом ROEMMI устанавливается аппаратный ключ DONGLE, выполненный на PIC-контроллере типа 16F876. Благодаря этому ключу (и программному обеспечению ZULEA) с помощью бокса ROEMMI можно, например, дополнительно считывать содержимое FLASH-памяти телефона (когда как полный EMMIBOX может только записывать данные в память). Более подробно на функциональных возможностях этих боксов мы останавливаться не будем, отметим лишь, что каждый из них имеет свои достоинства и недостатки.

Принципиальная схема аппаратного ключа показана на рис. 7.7.

Прошивка PIC-процессора для аппаратного ключа приведена на рис. 7.8.

Программирование аппаратов LEGACY в тестовом режиме

Существует два способа инженерного программирования телефонов LEGACY: с помощью тестового режима, и с помощью ПК через EMMIBOX.

Рассмотрим первый вариант более подробно.

Тестовое меню

Тестовое меню используется для изменения различных режимов работы телефона (в некоторых случаях — даже не свойственных для конкретной модели аппарата). Это объясняется тем, что ПО телефонов линейки LEGACY (например, в рамках конкретной серии) практически иден-

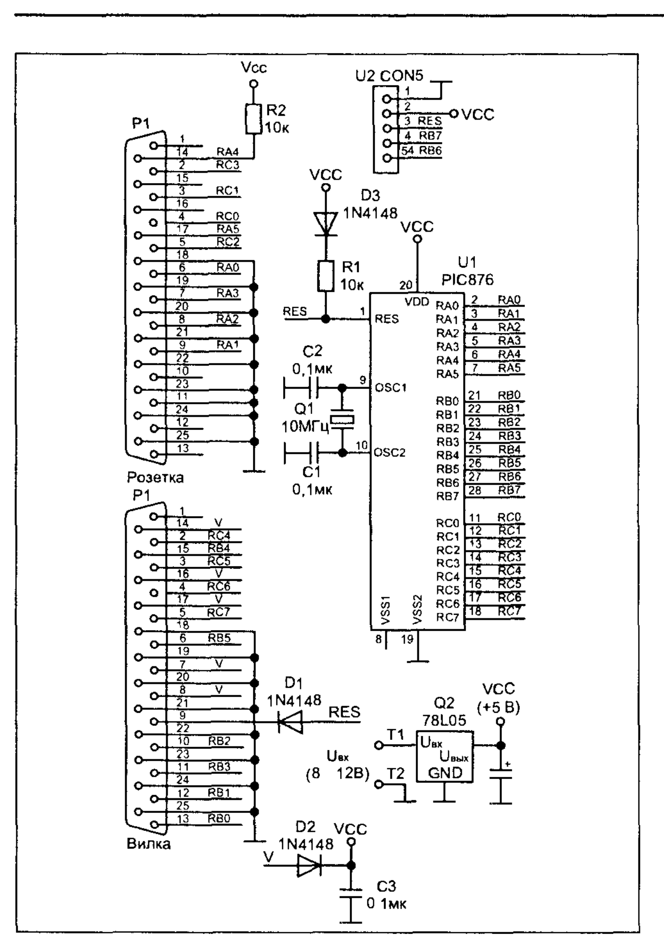


Рис. 7.7

тично. Отличия есть только в наборе пунктов основного меню аппарата. Тестовое меню позволяет корректировать этот набор и фактически менять функциональные возможности аппарата. В телефонах линейки LEGACY вход в тестовое меню осуществляется следующим образом: на клавиатуре телефона нажимают кнопку «#» и удерживают не менее 3 с. После этого на экране телефона должно появиться сообщение «Test». Если этого не произошло, для активации меню необходима специальная тестовая SIM-карта (Motorola Test Card) — эти карты до сих пор есть в свободной продаже. Выходят из тестового меню по команде 01#<OK>.

Перечислим основные команды тестового меню (всего команд около 100), которые могут понадобиться при ремонте аппаратов:

58# — отобразить SECURITY-код телефона (рис. 7.9);

58xxxxxx# — изменить SECURITY-код (xxxxxx — новый код). По умолчанию код имеет значение 000000;

59# — отобразить LOCK-код телефона (рис. 7.10);

59xxxx# — изменить LOCK-код (xxxx — новый код). По умолчанию код имеет значение 1234;

19# — отобразить версию ПО телефона (рис. 7.11). На рисунке видно, что версия ПО телефона —10-я (на порядке определения номера версии ПО мы останавливались выше);

Тестовые команды

Корректировкой содержимого регистров телефона можно менять его меню и основные функции, например, включать функцию виброзвонка, если она поддерживается аппаратно.

Отметим, что для изменения содержимого регистров телефона, используется следующий формат команд **???XXX?Y?<OK>**, где:

? — символ, который отображается на дисплее телефона, если нажать и удерживать кнопку «*» более 3 с;

XXX — номер регистра;

Y — содержимое регистра (0...9). Обычно используются 0 или 1 (включить/выключить).

При наборе этих команд телефон должен находиться в обычном режиме работы (входить в тестовое меню не нужно), но это относится только к тем аппаратам, в которых можно войти в тестовое меню без тестовой SIM-карты.

Приведем номера некоторых регистров (всего их около 300), а также функции, которые они активируют:

123 — отображение времени и даты. После ввода команды в расширенном меню появятся пункты установки времени и даты, а также формата времени. Необходимым условием для работы этого регистра является включение функции «Real Time Clock», которая активируется в тестовом меню командой 8801#<OK>;

000, 001 — включают возможность записи в регистры;

149 — включает отображение заряда аккумулятора на экране телефона;

168 — включает отображение мощности сигнала на экране телефона;

006 — включает полный показ разделов меню «Функции вызова» и «Сообщения»;

007 — включает полосу прокрутки в меню;

002 — включает возможность блокировки клавиатуры нажатием сочетания кнопок «*» и «#»;

104, 127 — «Телефонная книга»;

081 — включает функцию поиска записи по имени;

082 — включает функцию поиска записи по порядковому номеру;

092 — активирует меню «Функции вызова»

026 — изменяет пароль блокировки»

033 — активирует функцию «Широковещательная передача»;

```
02000000002FCF
10001000B6301822B6301822182F231223088600073
10003000182F231223088600093031221822OA3093
100050000D303122182 20E30312218220F30312279
100070000B30312218220C30312218220D3031225F
100090002522AB00231223088600 2522AC00231260
1000B000AE002312230886002522AF00231 2230856
1000D000231223088600 0930B8002B08B9005522E6
1000F000B90055220C30B8002E08B90055220D3039
1001100055220F30B8003108B90055225530182249
100130008600 2522AC002312230886002522AD006C
100150002522AF002312230886002522B00023 1297
10017000B8002C08B90055220C30B8002D08B90081
100190002F08B90055220F30B8003008B900552299
1001B0001822182F231223088600 05303122182216
1001D000231223088600 2522AB002B08013C0319BB
1001F0004B292B08043C03197529182F23122308B7
1002100018222A081822182F2312230886002522C4
100230008600 2522AD002312230886002522AE0069
1002500031D4629AA30AC02031D4629AE02031D28
1002700031D3E29AA0A031D3E2946292908A70075
100290002A081822182F2312230886002522AB00D3
1002B0002522AD002312230886002522AE0023123A
1002D000A7000030FD210030A7000130FD2155307E
1002F0002522AB002312230886002522AC002312FE
10031000AE002312230886002522AF0023122308F3
10033000231223088600 2522B20023122308 8600F8
10035000FD213008A7001130FD213108A70012301F
10037000AA301822182F83160313CF308500E030DF
10039000860187018B018C018D0108006430A1006A
1003B000D7292316230886000861ADC29070E0F3951
1003D000E7292316230886000861AEC2908008312D1
1003F0000C08831203 13A7000800831203178D0053
100410008C130C158B138B1B0A2A55308D00AA30B8
10043000A8000F39E2212312230886 00280E0F3965
10045000A800231223088600D721220EF039280491
10047000000085168316031 3CF308500FF308700F8
100490000F39B904051683160313C0308500F030F8
1004B0000F398700851200008516390EF038850047
1004D0000230B5002230B600E130B70008008312C8
1004F000EF212C082702031D8A2A1230EF212D0834
100510008A2A9E2A52302B02031D9B2A33302C023A
1005300031D9B2A9E2AAA30B30008005530B30041
100E0000BB21A30123088600F1308500F030870064
100E2000F1308500F0308700051685 16CE21662248
100E400005280D28182F182FE8281928322845289A
02400E000A0C9A
10421000FF00FF00FF00FF00FF00FF00FF00FF00A6
10423000FF00FF00FF00FF00FF00FF00FF00FF0086
10425000FF00FF00FF00FF00FF00FF00FF00FF0066
10427000FF00FF00FF00FF00FF00FF00FF00FF0046
10429000FF00FF00FF00FF00FF00FF00FF00FF0026
1042B000FF00FF00FF00FF00FF00FF00FF00FF0006
1042D000FF00FF00FF00FF00FF00FF00FF00FF00E6
1042F000FF00FF00FF00FF00FF00FF00FF00FF00C6
10431000FF00FF00FF00FF00FF00FF00FF00FF00A5
10433000FF00FF00FF00FF00FF00FF00FF00FF0085
10435000FF00FF00FF00FF00FF00FF00FF00FF0065
10437000FF00FF00FF00FF00FF00FF00FF00FF0045
10439000FF00FF00FF00FF00FF00FF00FF00FF0025
1043B000FF00FF00FF00FF00FF00FF00FF00FF0005
1043D 000FF00FF00FF00FF00FF00FF00FF00FF00E5
1043F000FF00FF00FF00FF00FF00FF00FF00FF00C5
080008000428231223088600DE
10002000340818223508182236081822370 81822F2
100040003122182 20B30312218220C30312218229 2
100060001822182F2312230886000A30312218226 2
1000800018220E303122182 2182F231223088600 3E
1000A000230886002522AD002312230886002522 7E
1000C0008600 2522B00023122308 86002522B100D5
1000E0000A30B8002C08B90055220B30B8002D0892
10010000B8002F08B90055220E30B8003008B900E9
10012000182F2312230886002522AB00231223 0850
10014000231223088600 2522AE002312230886 00EE
10016000230886000A30B8002B08B90055220B304E
1001800055220D30B8002E08B90055220E30B800A7
1001A0005530182 2182F231223088600013031 22DF
1001C000182F231223088600 0F3031221822182FEF
1001E000FE282B08023C03190C292B08033C031999
10020000860000 30EF21A9000130EF21AA00290863
10022000AB002312230886002522AC0023122308EA
10024000231223088600 5530AB02031D4629AD0258
10026000046290030EF21A9000130EF21AA00A90A98
100280000030FD212A08A7000130FD2129081822 8D
1002A000231223088600 2522AC00231223088600 8F
1002C000230886006F223308553C031D7229003035
1002E0001822182FAA301822182F2312230886004C
10030000230886002522AD0023122308860025221B
100320008600 2522B000231223088600 2522B10072
100340006F223308553C031DB8292F08A700103031
10036000FD213208A7001330FD2155301822182F27
100380008600FF308700F6309F00831203138501 3B
1003A000FF30A000A00BD229A10BD0290800861E87
1003C000A20008000F39A3002312230886 00861E0E
1003E00003178D00831603178C130C148312031745
10040000831203132708831203178C008316031724
100420008D008C148C18122A0C11831203130800EF
10044000E22123122308860008 00D72122080F3951
100460000800B800F130850038080F398700851280
100480008312031305120000050EF039B9000708A6
1004A00087008312031339080800F03085003808EC
1004C00039088700051200000516080000 30B40046
1004E000031 31030EF212B082702031D8A2A113035
100500002702031D8A2A1330EF212E082702031D1C
1005200031D9B2A47302D02031D9B2A02302E02F9
020540000800B1
100E1000831603 13C0308500F03087008312031 35C
100E30008312031 3D72107308A0022080F39820753
100E50009128D328DA28E128182F182F182F182FB7
104200000000000 0FF00FF00FF00FF00FF00FF00B4
10422000D20004000000000FF00FF00FF00FF00BC
10424000FF00FF00FF00FF00FF00FF00FF00FF0076
10426000FF00FF00FF00FF00FF00FF00FF00FF0056
10428000FF00FF00FF00FF00FF00FF00FF00FF0036
1042A000FF00FF00FF00FF00FF00FF00FF00FF0016
1042C000FF00FF00FF00FF00FF00FF00FF00FF00F6
1042E000FF00FF00FF00FF00FF00FF00FF00FF00D6
10430000FF00FF00FF00FF00FF00FF00FF00FF00B5
10432000FF00FF00FF00FF00FF00FF00FF00FF0095
10434000FF00FF00FF00FF00FF00FF00FF00FF0075
10436000FF00FF00FF00FF00FF00FF00FF00FF0055
10438000FF00FF00FF00FF00FF00FF00FF00FF0035
1043A000FF00FF00FF00FF00FF00FF00FF00FF0015
1043C000FF00FF00FF00FF00FF00FF00FF00FF00F5
1043E000FF00FF00FF00FF00FF00FF00FF00FF00D5
00000001FF
```

Рис. 7.8

243 — активирует функцию настройки контрастности дисплея;
179 — активирует функцию блокировки клавиатуры;
148 — вкл/выкл звонка;
138 — изменяет PIN2-код SIM-карты;
040 — регулирует громкости звонка;
041 — блокирует телефон;
043 — изменяет код разблокировки;
045 — изменяет PIN-код SIM-карты;
047 — включает расширенные меню;
048 — выбор языка меню;
154 — английский язык меню;
157 — немецкий язык меню;
229 — русский язык меню;
266 — украинский язык меню;
050 — изменяет приветствие;
051 — включает режим экономии батареи;
052 — выбор звукового сопровождения при нажатии кнопок;
055 — полный сброс телефона;
056 — полный сброс телефона с очисткой памяти;
094 — выбор сети;
203 — изменяет радиочастотный диапазон работы телефона;
253 — включает на диапазон 1900 МГц;
254 — включает на диапазон 900/1800 МГц;
204 — включает на диапазон 900 МГц;
205 — включает на диапазон 1800 МГц;
096 — включает раздел меню «Настройка аксессуаров». Этот раздел появится при подключении к телефону комплекта Handsfree и др.;
079 — автоматический выбор Handsfree.

Основные пакеты для программирования телефонов MOTOROLA LEGACY с ПК

Существует несколько основных пакетов для ПК, предназначенных для программирования телефонов MOTOROLA линейки LEGACY.

Работа с этими пакетами включает в себя:

— **флеширование** — «прошивку» основного ядра ПО (файл CP) и языковых пакетов (файл LP). Подобная процедура используется для смены версии ПО и изменения языковых пакетов. Процедура флеширования использует файлы с расширением *.hex (формата motorola) и *ebf (сжатый файл, наподобие архивного);
— **флексирование** — изменение содержимого настроечных таблиц, хранящихся в области EEPROM и включающих в себя все виды блокировки, коды телефонов, опции меню, записные книжки и др. (чаще всего эту процедуру используют для снятия SIM LOCK, восстановления IMEI-номера и др.). Процедура флексирования использует файлы с расширением *.fdf;
— собственно, программный ремонт аппаратов.

Удобство использования данных форматов файлов прошивки состоит в том, что содержимое файла можно редактировать в обычном БЛОКНОТЕ (из стандартных функций WINDOWS).

Рассмотрим основные программы для работы с телефоном линейки LEGACY, их особенности, а также порядок работы с ними.

Примечание. *При выполнении всех операций по программированию телефонов, аккумуляторные батареи аппаратов должны быть полностью заряжены*

Программа MotoFLEX

Одной из программ, работающей с полным боксом EMMI (EMMIBOX), является пакет MotoFLEX. Последняя версия этой программы — 8.6.

После установки программы MotoFLEX в корневом каталоге диска **C:/** появится директория MOTOSOFT. В нее необходимо скопировать все имеющиеся файлы «прошивки» телефонов.

Существует два способа флеширования телефона:

— за один этап, когда языковой пакет загружается одновременно с ПО — это файл, именуемый CP+LP;

Рис. 7.9

Рис. 7.10

Рис. 7.11

— два этапа, когда сначала загружается ПО (CP), а затем — языковой пакет LP.

Почти все телефоны линейки LEGACY могут быть запрограммированы (флешированы) в один этап, за исключением «Motorola V3690». Эта модель флешируется только в два этапа.

Перед тем, как приступить к описанию процедуры флеширования, необходимо отметить, что в зависимости от количества этапов программирования hex-файлы бывают несколько типов:

- **xx_xx_xx.hex** — файл, содержащий только с ПО без языкового пакета (используется для флеширования в два этапа);
- **xx_xx_xx_lang06.hex** — файл языкового пакета, в том числе с поддержкой русского языка (используется для флеширования в два этапа);
- **xx_xx_xx_rus.hex** — файл ПО совместно с языковым пакетом, в том числе и русскоязычным (используется для флеширования в один этап).

Процедура флеширования телефона в один этап

Процедуру флеширования телефона в один этап (прошивка ПО и языкового пакета одновременно) выполняют в следующей последовательности:

1. Подключают EMMIBOX к ПК, затем подают на бокс питание и нажимают кнопку RESET.
2. Запускают программу MotoFLEX. Окно программы после ее загрузки показано на рис. 7.12. После нажатия кнопки INITIALIZE в окне сообщений должна появиться надпись «Motorola FLASH Programmer Version 625010», где 625010 — версия ПО бокса (она может быть любой другой).
3. Нажимают кнопку LOAD FILE (она появится после завершения процесса инициализации). После этого окно программы примет вид, показанный на рис. 7.13. Затем нажимают кнопку 1 DOWNLOAD HEX/EXO (в позициях 2 и 3 галочки не ставят).
4. После этого появится окно (рис. 7.14), в котором показаны папки с файлами для загрузки. В нем выбирают модель телефона и версию программного обеспечения (например, используют путь

C:\motosoft\cd920cd930\B5_07_02\B5_07_02.hex).

Для флеширования ПО с одновременной установкой русскоязычного языкового пакета выбирают файлы, которые заканчиваются на «_rus.hex», например, для телефонов M-серии M3588/3688/3788/3888 — это файл

BE_11_14_rus.hex.

В аппаратах CD930, D520 и M3088 языковой пакет уже включен в «прошивку» и автоматически загружается вместе с ней.

5. Загружают выбранный hex-файл в память EMMIBOX — на это потребуется 3...4 мин (см. рис. 7.15). Под окном сообщений появится

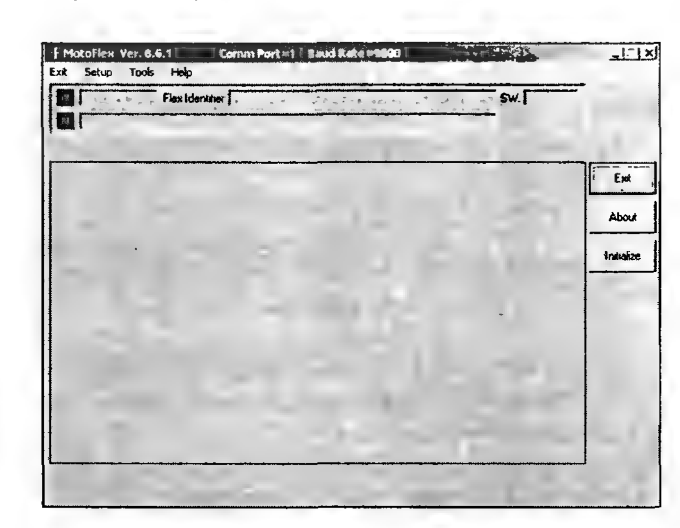


Рис. 7.12

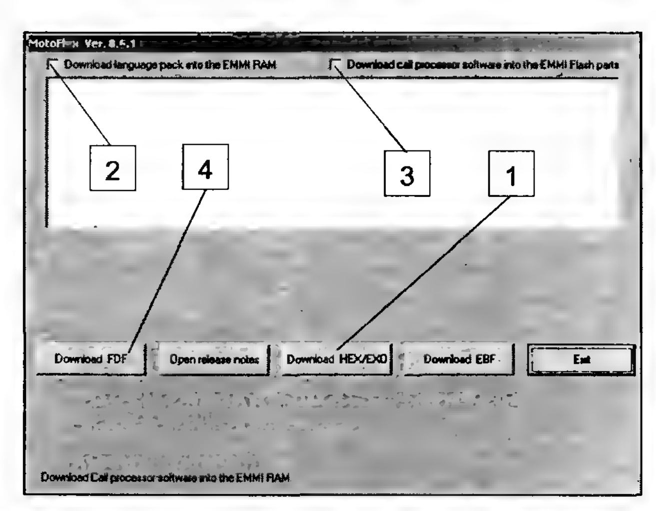


Рис. 7.13

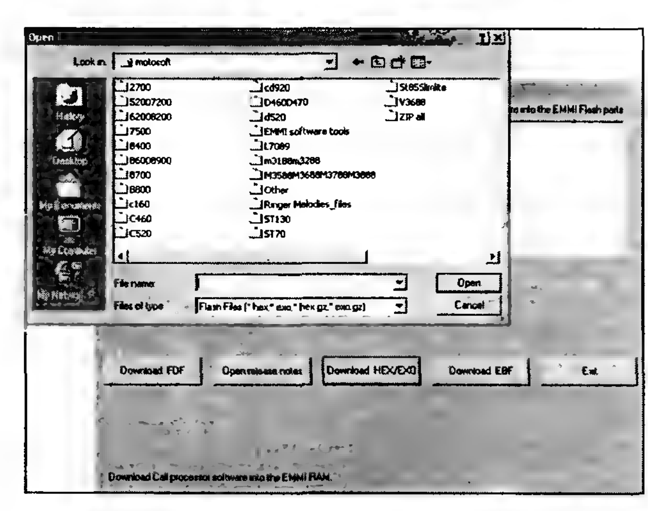


Рис. 7.14

шкала прогресса 1, с помощью которой можно контролировать процесс загрузки Красный индикатор на боксе во время загрузки должен мигать. Если он горит непрерывно — это свидетельствует об ошибке или какой-либо неисправности.

6. В конце загрузки появится окно с контрольной суммой (checksum) — см. рис. 7.16. После этого нажимают кнопку EXIT.
7. Подключают к EMMIBOX телефон и включают последний. На боксе должен загореться желтый индикатор.
8. Нажимают кнопку FLASH PHONE (1 на рис. 7.17). Процедура флеширования телефона с бокса будет длиться 25...40 сек Подобную процедуру нельзя прерывать, так как это может привести к выходу из строя телефона. В конце операции появится контрольная сумма, телефон после этого автоматически выключится.
9. Процедура флеширования закончена. Окно программы в этом случае будет иметь вид, показанный на рис. 7.18.
10. Необходимо открыть пункт выбора русского языка в меню телефона. Для активации Восточно-Европейских языков необходимо профлексировать (об этой процедуре мы остановимся ниже) аппарат (например, для cd930) файлом, находящимся в:

C:\motosoft\cd920cd930\B5_07_02\cd930_rus.fdf.

Отметим, что некоторые телефоны (V3688/3690) для открытия пунктов меню не требуют дополнительного флексирования.

Процедура флеширования телефона в два этапа

Процедура флеширования в два этапа (с дополнительной установкой языкового пакета), в отличие от предыдущей, имеет несколько отличий. Остановимся на них подробнее.

1. Выполняют шаги 1-3 из предыдущей процедуры.
2. Загружают файл

C:/motosoft\M3588M3688M3788M3888\be_10_34\BE_10_34.he.

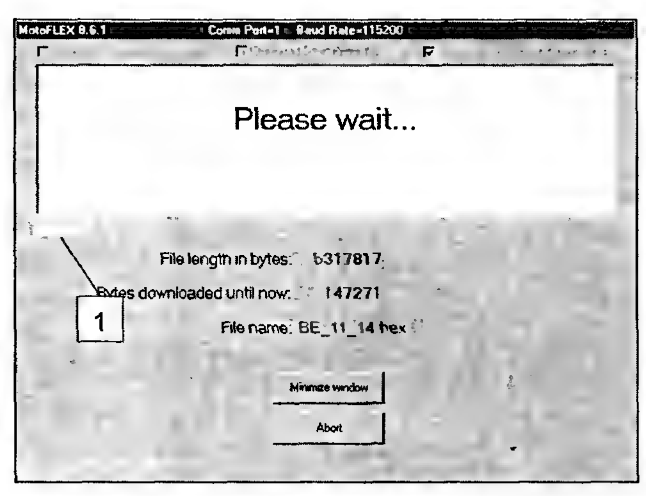


Рис. 7.15

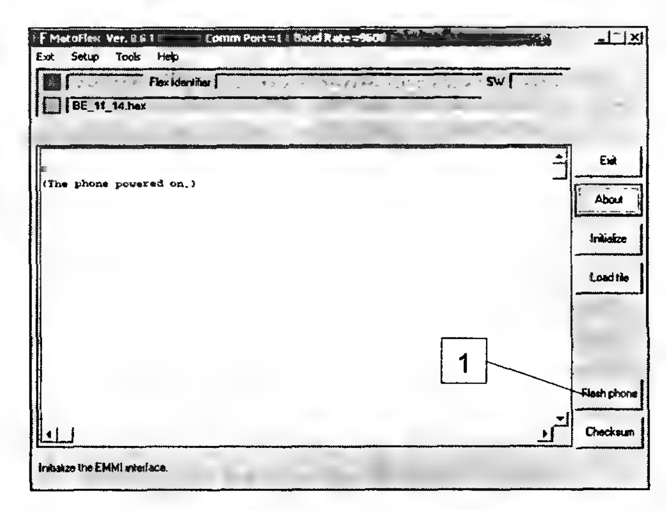


Рис. 7.17

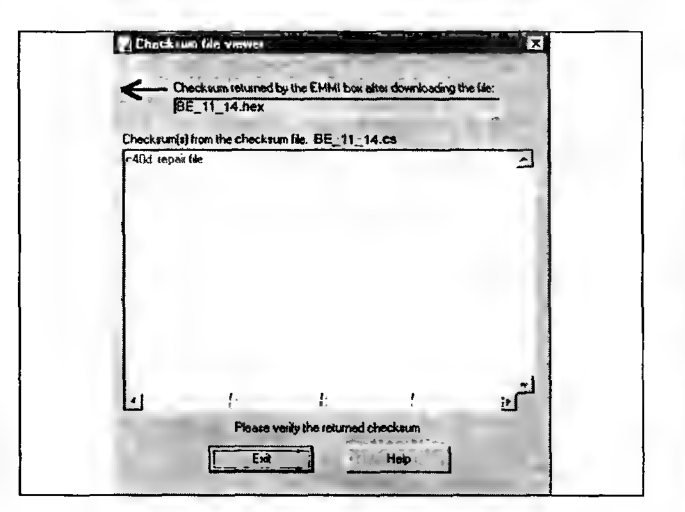


Рис. 7.16

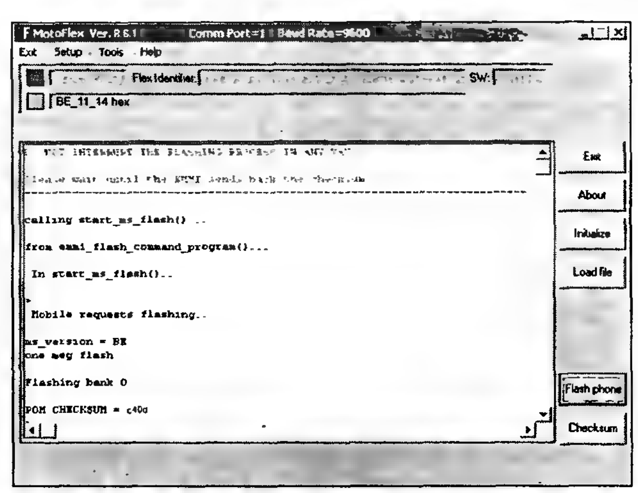


Рис. 7.18

Отметим, что если телефон имеет одинаковую версию ПО (что и раньше), необходимо «прошить» его снова для стирания уже существующего языкового пакета.

3. Соединяют бокс с телефоном и включают последний.
4. Нажимают кнопку FLASH PHONE. Дожидаются завершения процедуры флеширования (телефон после этого выключится).
5. Нажимают кнопку DOWNLOAD FILE и ставят галочку в поз. 1 — «Download language pack into the EMMI RAM» (рис. 7.19).
6. Нажимают кнопку DOWNLOAD HEX/EXO и выбирают необходимый языковый пакет.
7. Загружают hex-файл в бокс — эта операция займет 15...30 сек. Красный индикатор на боксе во время загрузки должен мигать.

Примечание. *Названия некоторых пакетов, соответствующих определенным наборам языков*

Language Pack 05 — датский, английский, французский, немецкий, гречеческий, венгерский, итальянский, португальский, испанский, турецкий,

Language Pack 06 — датский, английский, эстонский, финский, латвийский, литовский, норвежский, русский, шведский, украинский,

Language Pack 07 — болгарский, хорватский, чешский, английский, немецкий, польский, румынский, сербский, словенский, словацкий

8. Включают телефон (он должен быть подключен к боксу).
9. Нажимают кнопку FLASH PHONE. Процедура записи языкового пакета из бокса непосредственно в телефон обычно длится 10...15 сек (после завершения процедуры в окне программы появится контрольная сумма и аппарат автоматически выключится). Установка языкового пакета завершена.

Проконтролировать установку языкового пакета можно в тестовом режиме (Test Mode): языковый пакет — командой 193#, а версию ПО — 19#.

Если по окончании процедуры установки языкового пакета в меню телефона не появится новый пункт, например, русского языка, необходимо дополнительно профлексировать аппарат с помощью fdf-файла из соответствующей директории (об этом мы остановимся ниже).

Процедура флексирования телефона при снятии блокировки (LOCK)

Рассмотрим последовательность операций флексирования телефона при снятии блокировок.

1. Выполняют пункты 1-2, как описано в процедуре флеширования телефона в один этап.
2. Нажимают кнопку LOAD FILE (она появится после завершения процесса инициализации).

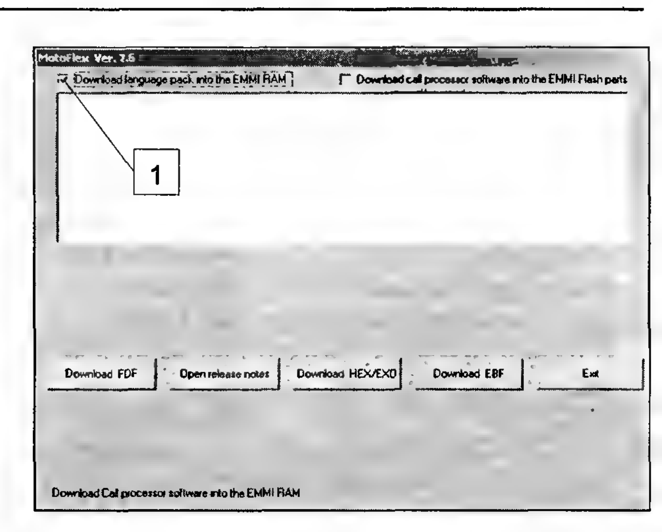


Рис. 7.19

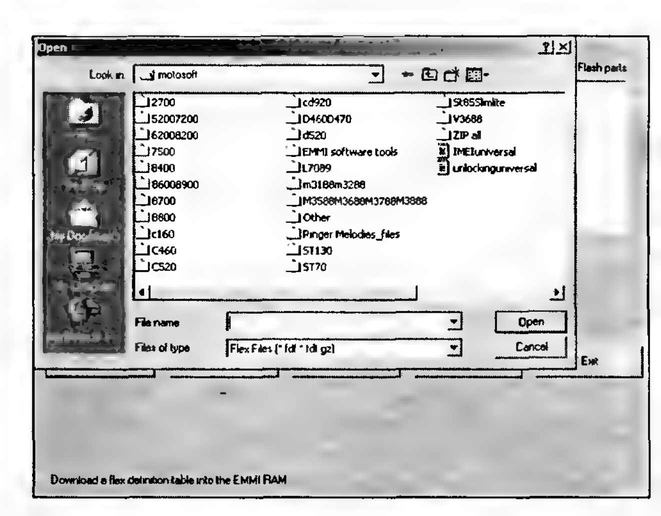


Рис. 7.20

После этого окно программы примет вид, показанный на рис. 7.13. Затем нажимают кнопку 4 DOWNLOAD FDF (в позициях 2 и 3 галочки не ставят).

3. После этого появится окно (см. рис. 7.20), в котором показаны папки с файлами и отдельные файлы. В нем выбирают файл **unlockinguniversal.fdf**.
4. Подключают к EMMIBOX телефон и включают последний. На боксе должен загореться желтый индикатор, окно программы при этом должно иметь вид, показанный на рис. 7.21.
5. Нажимают кнопку FLEX PHONE (1 на рис. 7.21).

После успешного выполнения процедуры флексирования программа отображает окно, показанное на рис. 7.22. После этого устанавливаются заводские значения кодов защиты телефона (SECURITY=000000; LOCK=1234). Если сообщение «Flexing Complette» не появляется в течении длительного времени (подобная ситуация встречается в модели телефона M3588 с версией ПО **C3_11_09**), выключают телефон и, под-

ключив к нему зарядное устройство, повторяют процедуру флексирования, начиная с пункта 2.

Процедура флексирования телефона при восстановлении IMEI-номера

1. Открывают при помощью программы NOTEPAD (Блокнот) файл **imeiuniversal.fdf**, находящийся в директории **motosoft.** Окно этой программы показано на рис. 7.23.
2. Элемент «@ seem 12:1» — это IMEI номер (swap byte nibbles), где:

код 08 4A 84 11 09 87 65 43 21 соответствует IMEI 448119078563412 (нужно лишь переставить между собой цифры в группах по две (или полубайты)).

Первые три цифры из исходного кода (80 A) — это длина (8 символов), а другие 15 цифр — IMEI (как уже отмечалось, этот номер соответствует оригиналу после перестановки цифр).

3. Считав исходный IMEI с наклейки аппарата, восстанавливают его значение в окне программы.
4. Сохраняют измененный файл, а затем загружают файл **imeiuniversal.fdf** и флексируют телефон аналогично процедуре при снятии блокировки (изменив лишь в нашем случае файл **unlockinguniversal.fdf** на **imeiuniversal.fdf**). Окно программы после проведения успешной операции восстановления IMEI-номера показано на рис. 7.24.

Другие процедуры флексирования

Обычно телефоны Motorola M-серии поступает на рынок с выключенной функцией часов.

Для выполнения этой функции флексируют аппараты следующими файлами:

— **c:\moto-soft\M3588_3688_3788_3888_rus_clock.fdf** (для телефонов с графическим дисплеем);
— **c:\motosoft\M3188_3288_rus_clock.fdf** (в версии с текстовым дисплеем).

Отметимследующие особенности:

— файлы **ptm_on.fdf** и **ptm_off.fdf** позволяют включать и выключать режим **Permanent Test Mode** (тестовый режим);
— файл **lifeclr.fdf** позволяет сбросить lifetimer телефона;
— файл **lock.fdf** позволяет установить SP LOCK, снятый ранее.

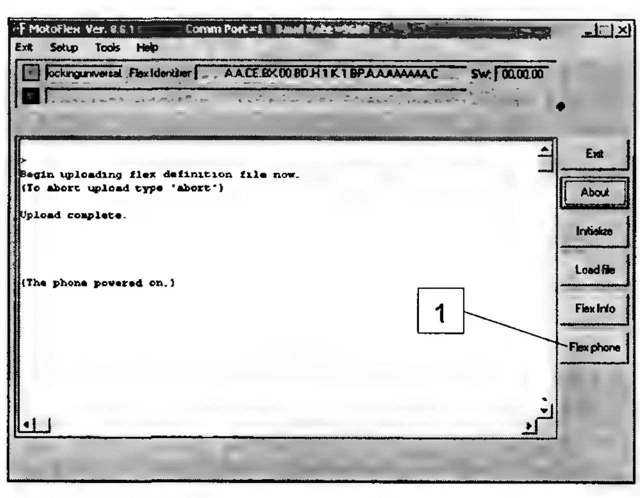
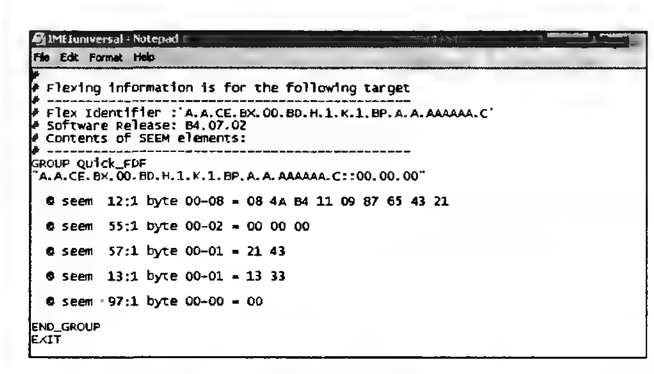


Рис. 7.21




```
#
# Flexing information is for the following target
# ------------------------------------------------
# Flex Identifier :'A.A.CE.BX.00.BD.H.1.K.1.BP.A.A.AAAAAA.C'
# Software Release: B4.07.02
# Contents of SEEM elements:
# ------------------------------------------------
GROUP Quick_FDF
"A.A.CE.BX.00.BD.H.1.K.1.BP.A.A.AAAAAA.C::00.00.00"
  @ seem  12:1 byte 00-08 = 08 4A B4 11 09 87 65 43 21
  @ seem  55:1 byte 00-02 = 00 00 00
  @ seem  57:1 byte 00-01 = 21 43
  @ seem  13:1 byte 00-01 = 13 33
  @ seem  97:1 byte 00-00 = 00
END_GROUP
EXIT
```

Рис. 7.23

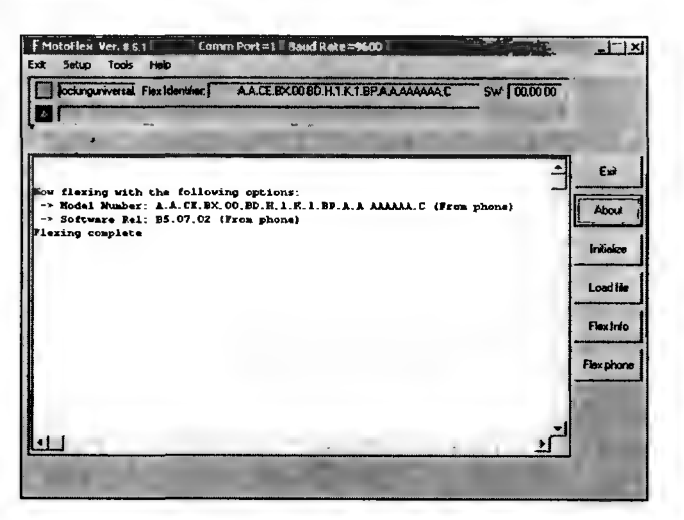


Рис. 7.22

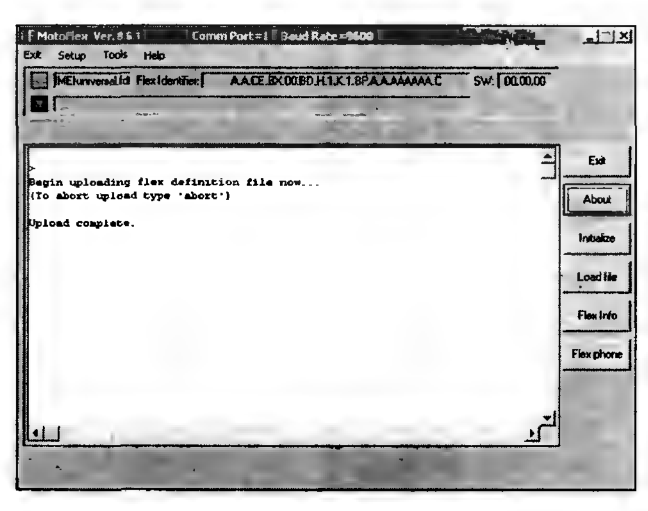


Рис. 7.24

Решение возможных проблем при программировании телефонов с помощью программы MotoFLEX

При загрузке hex- или ebf-файлов отображается ошибка и бокс не подсчитывает контрольную сумму «checksum» (красный индикатор на боксе может мигать совершенно произвольно)

Отсоединяют кабель от телефона, а затем заново загружают файл в EMMIBOX.

Отметим, что подобные случаи возникают, если производится загрузка файлов от ПК в бокс при подключенном к EMMIBOX телефоне.

При загрузке hex- или fdf-файлов могут возникнуть ошибки «RUNTIME ERROR 380» или «FILESIZE-1 ERRORS»

Подобные ошибки появляются, если указанные файлы имеют атрибуты READ ONLY или ARCHIVE, поэтому для устранения проблемы снимают все атрибуты с fdf-, hex- и ebf-файлов.

Невозможно загрузить hex-файл с ПК в EMMIBOX

Обычно эта проблема возникает при загрузке файла B5_07_02.

Для устранения проблемы необходимо отключить режим автоматического выбора, как показано на рис. 7.25.

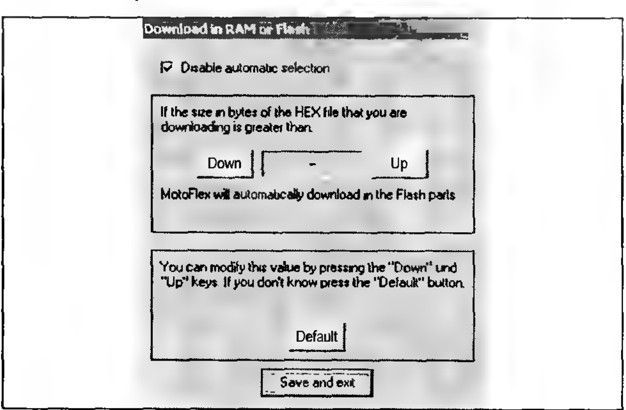


Рис. 7.25

Программа MotoKEY

Программа MotoKEY (в отличие от MotoFLEX, работающая совместно с EMMIBOX) предназначена для работы с боксом ROEMMI через аппаратный ключ DONGLE. Отличительные особенности этого программно-аппаратного комплекса следующие:

- в боксе ROEMMI отсутствует буферная память, поэтому файлы для программирования телефонов передаются непосредственно от ПК в телефон и запись файлов в телефон можно производить в один этап (а не как раньше: вначале от ПК в бокс, а затем — с бокса в телефон);
- связь между ПК и боксом производится через порт LPT, тем самым значительно ускоряется обмен данными, как в случае с полным EMMIBOX через COM-порт;
- позволяет читать файлы из FLASH-памяти телефона (что было невозможно при работе с EMMIBOX под управлением программы MotoFLEX);
- позволяет выполнять основные операции флексирования в один этап (для этого в окне программы есть соответствующие функциональные кнопки);
- позволяет устранять ошибки при неправильном программировании телефона (например, при неправильной разблокировке и др.);
- создавать свои собственные файлы CP (ПО) и LP (языковый пакет) из считанного flash-файла;
- понижать версию ПО и другие возможности.

Программа MotoKEY была создана компанией ZULEA (Daniel Henzulea).

Окно программы MotoKEY показано на рис. 7.26. Последняя версия программы — 9.7.

Следует отметить, что программа MotoKEY совместима только с боксами ROEMMI, работающими с программами pemaster, roemmi.exe версии 2.0 (под MS-DOS — см. рис. 7.27) или Win_emmi.exe версии 1.04 (см. рис. 7.28). Перечисленные программы входят в комплект постав-

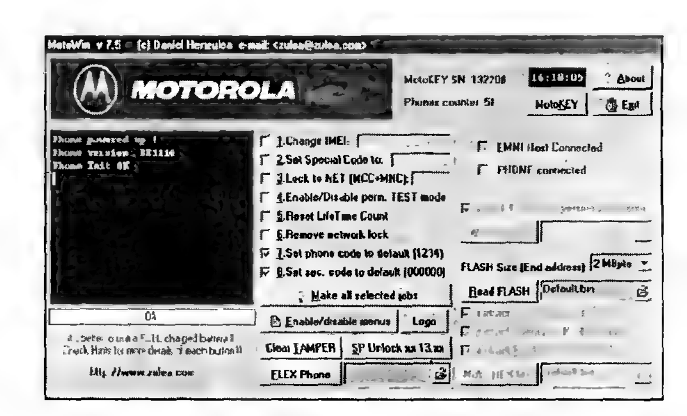


Рис. 7.26

```
RoEmmi Controler v2.0.
r - read lock from slave phone
u - unlock slave phone
l - lock slave phone
f - flash slave phone
i - imei change on slave phone
q - quit EMaster

Emmi Host connected
Phone disconected
Wait connection to emmi host
Emmi Host connected
Wait connection to slave phone
Phone connected
MASTER?>_
```

Рис. 7.27

Рис. 7.28

ки бокса, но по своим возможностям значительно уступают MotoKEY.

Рассмотрим основные возможности программы MotoKEY.

Прямые функции программы MotoKEY

Прямые функции программы MotoKEY — это операции, наиболее часто используемые с оригинальным ROEMMIBOX, которые в обычном варианте выполняются путем сложной последовательности операций по редактированию и загрузки FLEX-файлов (например, в формате fdf).

Программа MotoKEY позволяет выполнять сложные операции по программированию телефона в один этап. Перечислим эти операции:

- изменение (восстановление) IMEI-номера;
- установка специального кода;
- установка (снятие) блокировки сети (MNC и MCC);
- установка (снятие) постоянного тестового режима;
- сброс счетчика общего времени функционирования телефона,
- удаление кода сети (SP LOCK);
- установка кода телефона на значение по умолчанию — 1234;
- установка защитного кода на значение по умолчанию — 000000.

Фрагмент окна программы с этими функциями показан на рис. 7.29.

Отметим, что для выполнения выбранных операций, необходимо их пометить соответствующим флажком, а затем нажать кнопку MAKE ALL SELECTED JOBS (1 на рис. 7.26).

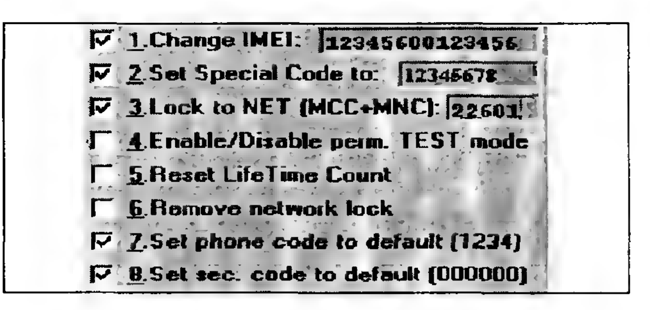


Рис. 7.29

Также следует учесть, что при выполнении прямых функций, выключенный телефон подключают к боксу, а уже затем включают (в противном случае все флажки и кнопки в окне программы не будут активны).

Процедура флексирования телефона

Процедура флексирования телефона включает в себя изменение содержимого настроечных таблиц, хранящихся в области EEPROM и находящихся в файлах Flex с расширением fdf. (Flex Definition Files).

При помощи этой процедуры можно изменить заставку при включении телефона, включать/отключать пункты меню, изменять различные параметры и др.

Информация по назначению некоторых областей памяти EEPROM приведена в табл. 7.1.

Таблица 7.1

Шестнадцатеричный адрес (в скобках — название области памяти EEPROM)	Функции
0C(SEEM 12)	IMEI-номер
0D(SEEM 13)	Флаги (0333 – тестовый режим выключен, 1333 – тестовый режим включен)
0E(SEEM 14)	Настройки клавиатуры и пунктов меню (122 байтов)
10(SEEM 16)	Область графического логотипа при включении телефона
37(SEEM 55)	Защитный код (по умолчанию – 000000)
39(SEEM 57)	Код блокировки (по умолчанию 2143, после перестановки полубайтов – уже знакомые 1234)
4B(SEEM 75)	Телефонная книга (100 записей)
61(SEEM 97)	Флаг SP LOCK (00 – без SP LOCK)
6D(SEEM 109)	Специальный код

Для флексирования телефона сначала необходимо выбрать нужный fdf-файл кнопкой 1 (рис. 7.30), а затем нажимают кнопку FLEX PHONE.

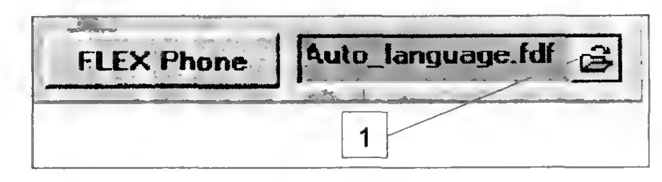


Рис. 7.30

Отметим, что после выполнения этой операции выключенный телефон подключают к боксу, а уже затем включают (в противном случае кнопка FLEX PHONE и поле имени файла (справа на рис. 7.30) не будут активны).

Процедура флеширования телефона

Флеширование аппарата подразумевает прошивку ядра ПО (замену версии на аналогичную, а также более позднюю или раннюю) и замену языковых пакетов.

Отметим, что при выполнении операции флеширования в телефоне должна отсутствовать SIM-карта.

В зависимости от выполняемой операции флеширования hex-файлами (CP, LP, CP+LP) для смены ПО необходимо иметь все три перечисленных типа файлов, а для замены только языкового пакета — только LP (но той же версии, что и CP-файл, уже записанный в телефон).

Из имени hex-файла можно понять, что в нем содержится. Кроме того, основным отличием всех LP-файлов от остальных является то, что они имеют меньший объем.

Также для определения типа файла, можно посмотреть его содержимое с помощью программы просмотра текста.

В этом случае можно увидеть соответствующие наборы символов (рис. 7.31 и 7.32).

На рисунках интересна вторая строка. Если после Sxxx (4 символа) расположены символы 0040A000 (как в первом примере) или 00006000 — это файл «прошивки ПО».

Если же во второй строке отображаются символы, отличные от приведенных (как во втором примере — 004D1110) — это языковый пакет. Символы в позициях 13-18 означают версию ПО телефона (BE1034), а с 19-20 указывают на версию самого языкового пакета (в нашем случае 05).

Можно поступить еще проще — версию ПО телефона можно определить в тестовом режиме с помощью команды #19, а командой #193 — версию языкового пакета. Кроме того, в тестовый режим можно войти из программы MotoKEY, установив в активное состояние флаг ENABLE/DISABLE PERMANENT TEST MODE.

Для флеширования телефона сначала выбирают нужный hex-файл кнопкой 1 (рис. 7.33), а затем нажимают кнопку WRITE FLASH и дожидаются сообщение о том, что нужно включить телефон. После этого включают телефон и контролируют состояние индикатора выполнения операции (до 98%). В этот момент телефон автоматически выключится и программа сообщит, что его снова нужно включить. Включают телефон и дожидаются состояния индикатора 100%, после этого появится сообщение «ALL FLASH OK».

Обычно процесс флеширования телефонов для файлов CP+LP занимает от 40 с до 3 мин (в зависимости от типа аппарата).

Отметим, что в случае прошивки только LP-файла в поле CHEK LANGPACK VERSION WITH PHONE нужно установить флажок. При прошивке файлов CP и CP+LP этот флажок устанавливать не нужно.

Процедура чтения FLASH-памяти телефона

Файл нужной версии ПО (или языкового пакета) можно считать и из другого исправного аппарата.

Процесс чтения FLASH-памяти состоит из трех шагов:

- выбирают размер FLASH-памяти;
- считывают Flash-память в специальный бинарный файл (формата BIN);
- извлекают, собственно, файлы CP, LP или CP+LP из бинарного файла.

Сам процесс чтения памяти телефона может занять от 1 до 3 часов.

Рассмотрим этот процесс подробнее.

Размер FLASH-файла выбирают в окне 1 (см. рис. 7.34). Если размер файла не известен, луч-

```
S00600004844521B
S3230040A000000000000DE2BEEFEA0282A0EA010A6FEA0301DEEA010A6DEA010A6CEA0174
и т д.
```

Рис. 7.31

```
S00600004844521B
S323004D1110BE103405004E22EC00000000004DADC800000000004D8F78004DCBC0004DD0
и т.д.
```

Рис. 7.32

Рис. 7.33

Рис. 7.34

ше выбрать больший (максимальное значение — 4 Мбайт). Ничего страшного в этом случае не произойдет, просто процесс чтения файла займет более длительное время.

В табл. 7.2 приведем размеры FLASH-памяти для некоторых моделей телефонов Motorola линейки LEGASY.

Таблица 7.2

Наименование модели	Размер Flash-памяти (Мбайт)
L2000, L7089	2
M3188, M3288	1
M3588, M3688, M3788, M3888	1
P6088, M6088	1
P7389	2
P7389 Asia	4
T180	1
T2288, V2288	2
T2288 Asia, V2288 Asia	4
V2088 Asia	1
V3688	1
V3888+ Asia	2
V3690	2
V50, V51	2
V8088 Asia	4

Вторым шагом будет выбор имени бинарного файла. Для этого нажимают кнопку 1 (рис. 7.35) и в поле слева вводят имя файла с расширением BIN, в котором будет сохранено содержимое Flash-памяти телефона. Затем нажимают кнопку READ FLASH и дожидаются, пока программа не выполнит операцию записи в файл *.BIN. После успешного завершения операции телефон автоматически отключится.

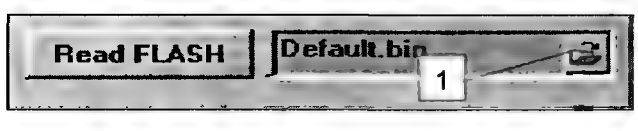


Рис. 7.35

Третьим шагом будет преобразование полученного бинарного файла в файлы CP, LP или CP+LP. Вначале отмечают флажками типы файлов (лучше выбрать все), которые необходимы (рис. 7.36).

Затем выбирают считанный заранее bin-файл и нажимают кнопку MAKE HEX FILES (см. рис. 7.37). После этого программа создаст вы-

Рис. 7.36

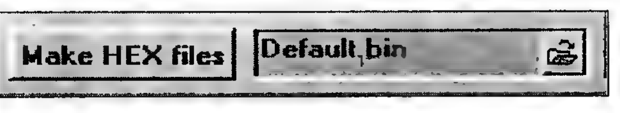


Рис. 7.37

бранные ранее файлы в той же папке, в которой находится и бинарный файл.

Процедура включения/выключения пунктов меню

Содержимое и пункты меню телефонов находятся в так называемой настроечной таблице (Flex Definition Table), хранящейся в области памяти EEPROM телефона.

Перед тем, как изменять выбранные пункты меню, вначале нужно прочитать эту таблицу из области SEEM 14 EEPROM (см. табл. 7.1). Делают это нажатием кнопки ENABLE/DISABLE MENUS (телефон перед этой операцией должен быть соединен с боксом и включен). Если при чтении из области EEPROM возникла ошибка, чаще всего бывает достаточно выключить и снова включить телефон.

При положительном завершении операции чтения появится новое окно с пунктами и полями для флажков (рис. 7.38). При необходимости устанавливают или снимают флажки в пунктах окна (фактически, эти флажки включают/выключают пункты меню телефона, а также режимы его работы). После выполнения всех необходимых изменений нажимают кнопку WRITE CHANGES — после этого новые изменения будут записаны в телефон.

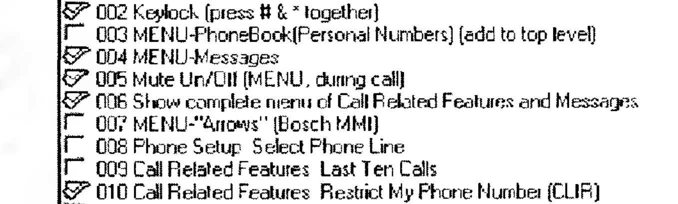


Рис. 7.38

Следует отметить, что при приведении подобной процедуры не следует включать функции, использующие аппаратное обеспечение, отсутствующее в данной модели телефона (это касается голосовых функций, виброзвонка, инфракрасного порта и др.) В худшем случае «экспери-

менты» с меню могут вывести телефон из строя (например, если активировать функцию VoiceNotes в аппарате T2288).

Процедура чтения/записи логотипа

Логотип заставки (Graphic Logo) хранится в области SEEM 16 EEPROM (см. табл. 7.1). Эту прошивку можно считать, при желании — отредактировать, а затем вновь записать в память телефона. Для этого соединяют бокс с телефоном и включают последний. Затем в окне программы нажимают кнопку LOGO. После этого будет произведено чтение области SEEM 16 из EEPROM.

Если при проведении этой операции возникла ошибка, чаще всего бывает достаточно выключить и снова включить телефон.

При положительном завершении операции чтения появится новое окно, показанное на рис. 7.39. На нем есть несколько кнопок, а также считанное изображение заставки из памяти телефона.

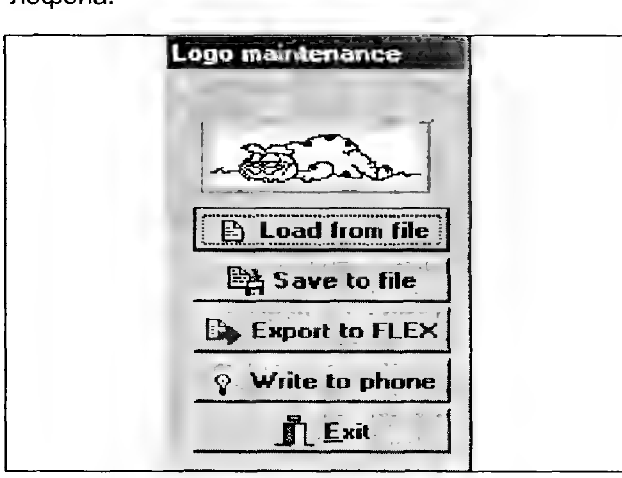


Рис. .7.39

Назначение кнопок этого окна следующее (сверху вниз на рис. 7.39):

- загрузить новое изображение из файла (формат Bitmap);
- сохранение считанного изображения (в формате Bitmap);
- экспорт считанного или загруженного изображения в формат PDF Flex;
- запись загруженного изображение в память телефона;
- выход без сохранения.

Процедура снятия состояния TAMPER ALERT

Версии прошивок телефонов C4_13_03, DB_13_03, F0_13_03 и AF_7F_C7 имеют следующую особенность: любые попытки разблокировать телефоны с этими прошивками при помощи полного EMMIBOX и некоторых вариантов ROEMMI (без ключа DONGLE) приведет к тому, что аппарат автоматически перейдет в режим TAMPER ALERT.

Для разблокировки телефонов с этими версиями ПО, выполняют следующие действия:

1. Вставляют в телефон SIM-карту, соединяют его с боксом, а затем включают телефон.
2. Если аппарат перейдет в режим TAMPER ALERT, нажимают кнопку CLEAR TAMPER. Телефон отключится, но при следующем включении запросит специальный код (SPECIAL CODE). Если режим TAMPER ALERT опять будет активирован, заново повторяют этот пункт.
3. После запроса специального кода нажимают кнопку SP UNLOCK xx.13xx, и, после того, как программа выведет сообщение «DONE», вводят код 00000000#. На экране телефона должно появиться сообщение «COMPLETED». Выключают телефон, а затем вновь включают — он должен быть разблокирован. Если на экране телефона появится сообщение «WRONG CODE» (неверный код), вводят еще раз код. Если и в третий раз аппарат будет запрашивать специальный код, снова повторяют пункт 3.
4. Если на экране телефона появится сообщение «WAIT TO ENTER SPECIAL CODE» (ожидание ввода специального кода), переводят аппарат в режим TAMPER ALERT путем флексирования файлом tampert.fdf, а затем переходят к пункту 2.

Отметим, что при выполнении данной процедуры в некоторых случаях требуется многократное повторение пунктов 2 и 3. Это обычно случается, если ранее были предприняты попытки разблокировки телефонов с помощью полного бокса EMMI и бокса ROEMMI (без DONGLE). Повтор пунктов 2 и 3 должен окончательно решить подобную проблему.

Другие пакеты для программирования телефонов Motorola линейки LEGACY

Для программирования телефонов Motorola линейки LEGACY существуют еще несколько полезных программ, одна из них — GUI EMMI. Окно этой программы показано на рис. 7.40.

Программа GUI EMMI позволяет выполнять большинство операций, что и программа MotoFLEX (но не весь набор). Основное отличие этой программы заключается в том, что операции программирования телефонов выполняются через прямые опции меню (например, восстановление IMEI, выполнение разблокировки, активация тестового режима, выполнение полного программного сброса телефона, эмуляцию нажатия

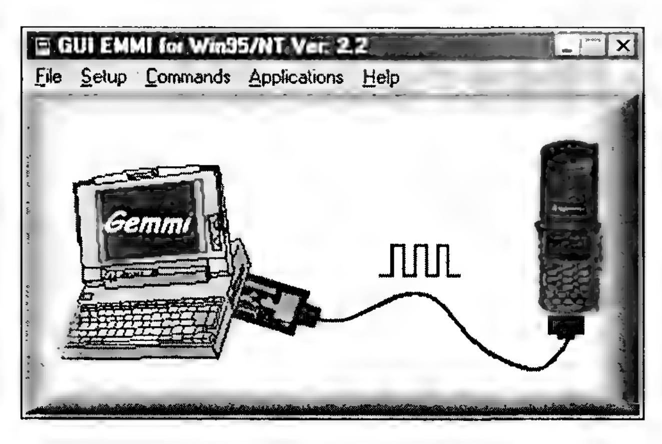


Рис. 7.40

различных кнопок на клавиатуре телефона, создание новых мелодий и др.).

Следующая интересная программа называется GSM KEYPAD SIMULATOR. Ее окно показано на рис. 7.41. Это, собственно, клавиатурный симулятор, который кроме своей основной функции, позволяет выполнять, например, операции флеширования или флексирования, контролировать и настраивать параметры радиочастотных блоков телефонов, а также многое другое.

Данные программы работают только с полным EMMIBOX (EMMI 2D).

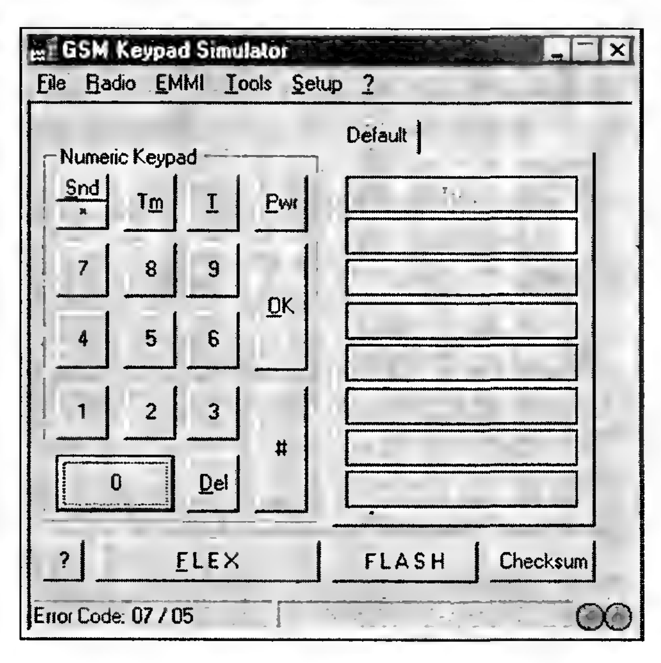


Рис. 7.41

Программный ремонт телефонов линейки LEGACY в случаях невозможности их включения

Особенностью работы телефонов линейки LEGACY совместно с боксами EMMI является то, что если телефон не включается (не стартует его управляющая программа, при условии, что аппаратная часть исправна), все действия по его программированию (флешированию, флексированию и др.) невозможны.

В этом случае поступают следующим образом

Вначале создают так называемый ремонтный (REPAIR) файл, содержащий в себе полные данные Flash-памяти телефона (так называемый FULL FLASH).

Затем телефон принудительно переводят в режим FLASH MODE. Для этого на вывод CS0 микросхемы FLASH-памяти аппарата подают лог 1 (от «+» шины питания телефона через ограничительный резистор номиналом 1 кОм), нажимают кнопку включения аппарата и снимают временный «щуп» с вывода микросхемы памяти. После этого телефон включится, а затем автоматически запускается процесс флеширования (естественно, предварительно в бокс уже должна быть записана «прошивка» с «ремонтным» файлом и дана команда на запуск процесса флеширования) После программирования телефона REPAIR-файлом, телефон уже должен включиться обычным образом. Однако многие его функции и режимы могут не удовлетворить пользователя (может отсутствовать нужный языковый пакет, аппарат может быть заблокирован и др.), но это не страшно — важно, что с телефоном уже можно работать. После этого программируют телефон обычным образом (флешируют, флексируют и др.).

Следует отметить, что во всех телефонах линейки LEGACY вывод CS0 микросхемы Flash-памяти выведен на контрольные точки — TEST POINT. Расположение этих точек для некоторых типов аппаратов LEGACY показано на

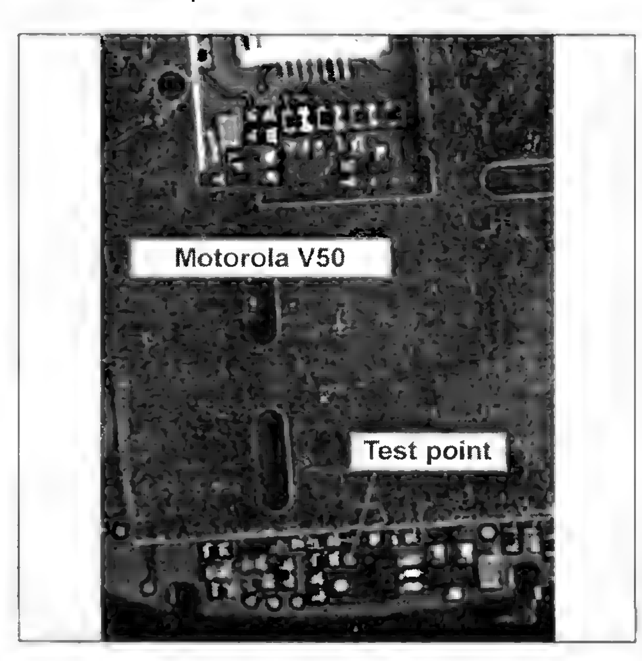


Рис. 7.42

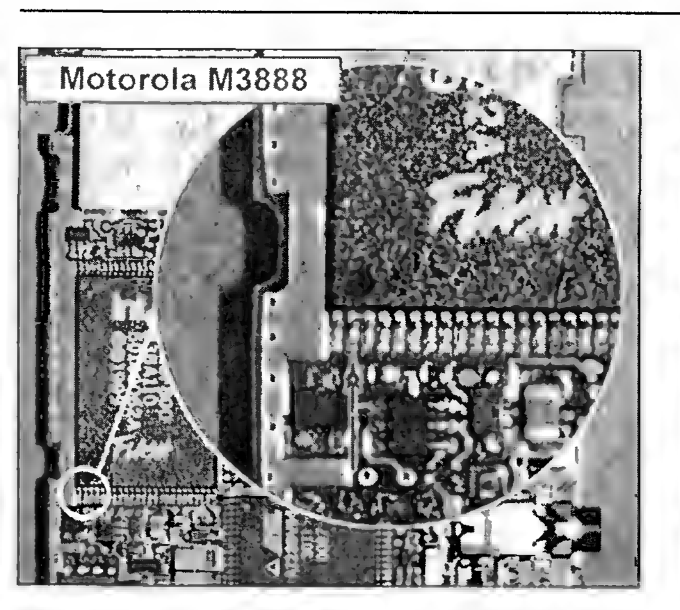


Рис. 7.43

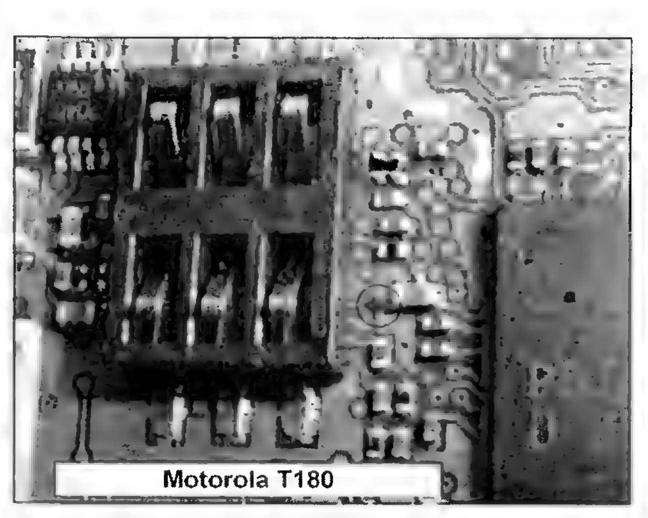


Рис. 7.44

рис 7.42—7.44. Расположение точек для других моделей можно поискать в Интернете.

Таким же способом можно произвести понижение версии аппарата — с xx.13.xx или xx.14.xx на xx.10.xx (при наличии ремонтного файла) Это необходимо для проведения разблокировки, если версия EMMIBOX (ROEMMIBOX) не поддерживает работу со «старшими» версиями ПО.

Глава 8. Сотовые телефоны NOKIA

Общие сведения

Сотовые телефоны NOKIA выпускаются на нескольких платформах Первые платформы телефонов назывались DCT-1 и DCT-2, а более поздние — DCT-3, DCT-4, DCT-L (коммуникаторы), WD-2 (смартфоны).

Соответствие некоторых поколений телефонов NOKIA их коммерческим (и сервисным) наименованиям (моделям) приведено в табл. 8.1.

В этой главе в основном пойдет речь о телефонах, выполненных на платформах DCT-3 и DCT-4.

Платформу DCT-3 объединяют следующие практически идентичные компоненты: микропроцессор (CPU) поколения MAD2, сигнальный процессор COBBA и микросхемы EEPROM, RAM и FLASH-памяти. Память может быть реализована в отдельных микросхемах, например, в «Nokia 3210» — это три разные микросхемы, в «Nokia 3310» — две, а в «Nokia 8210» — вообще одна.

Необходимо отметить, что все аппараты, выполненные на платформе DCT-3, имеют только монохромный дисплей.

Компания NOKIA всегда очень трепетно относилась к защите программного обеспечения своих телефонов, и поэтому многие ремонтники до недавнего времени при прошивке содержимого FLASH-памяти этих телефонов испытывали опре-

Таблица 8.1

Наименование платформы	Коммерческое (сервисное) наименование моделей Nokia
DCT-1	1011,1610, 1611, 1630, 1631, 2110, 2010, 2110i, 2118, 2120, 2140, 2148, 2148i, 2160, 2170, 2180, 2190, 6050, 6080, 6081, 9000, 9000i
DCT-2	3110, 8110, 8110i, 8146, 8148, 8148i
DCT-3	2100 (NAM-2), 3210 (NSE-8), 3285/3310 (NHM-5), 3320/3330 (NHM-6), 3350 (NHM-9), 3360/3390 (NPB-1), 3395/3410 (NHM-2), 3610 (NAM-1), 3810, nk402/nk503/nk702/5110 (NSE-1), 5110i (NSE-2), 5120/5125/5130 (NSK-1), 5148/5160/5165/5170/5180/5185/5190/5210 (NSM-5), 5510 (NPM-5), 5190 (NSB-90), 6090 (NME-3), 6110 (NSE-3), 6110i/6120/6130 (NSK-3), 6138/6150 (NSM-1), 6150e/6160/6161/6162/6185/6188/6190 (NSB-3), 6210 (NPE-3), 6250 (NHM-3), 7110 (NSE-5), 7160/7190/8210 (NSM-3), 8250 (NSM-3D), 8260/8270/8290 (NSB-7), 8810 (NSE-6), 8850 (NSM-2), 8855 (NSM-4), 8860/8890 (NSB-6), 9110 (RAE-2)
DCT-4	1100 (RH-18), 1100A (RH38), 1100B (RH-36), 1220 (NKC-1), 1260/1261 (NKW-1), 2112 (RH-57), 2220 (RH-40), 2221 (RH-42), 2260 (RH-39), 2261 (RH-41), 2270 (RH-3P), 2275 (RH-3DNG), 2280 (RH-17NA), 2285 (RH-3), 2300 (RM-4), 2300A (RM-5), 2600 (RH-59), 2600CN (RH-60), 2650 (RH-53), 2651 (RH-54), 3100/3120 (RH-19), 3100B (RH-50) 3105 (RH-46/48), 3108 (RH-6), 3125 (RH-61), 3200 (RH-30), 3200B (RH-31), 3205 (RM-11), 3220 (RH-37), 3220B (RH-49), 3300 (NEM-1), 3300B (NEM-2), 3320 (NPC-1), 3360 (NPW-1), 3510 (NHM-8), 3510i (RH-9), 3520 (RH-21), 3560 (RH-14), 3570i (NPD-4FW), 3585 (NPD-4), 3585i (NPD-4AW), 3586i (RH-44), 3590 (NPM-8), 3595 (NPM-10), 5100 (NPM-6), 5100A (NPM-6X), 5140 (NPL-5), 5140B (NPL-4), 6012 (RM-20), 6015/6016/6019 (RH-55), 6020 (RM-30), 6020B (RM-31), 6021 (RM-94), 6100 (NPL-2), 6011i (RH-58), 6101 (RM-76), 6102 (RM-77), 6108 (RH-4), 6170 (RM-47), 6170B (RM-48), 6200 (NPL-3), 6220 (RH-20), 6225 (RH-27), 6230 (RH-12), 6230B (RH-28), 6230i (RM-72), 6255/6256 (RM-19), 6310 (NPE-4), 6310i (NPL-1), 6340, 6340i (RH-13), 6360 (NPW-2), 6370 (NHP-2FX), 6385 (NHP-2AX), 6500/6510 (NPM-9), 6560 (RH-25), 6585 (RH-34), 6590 (NSM-9), 6610 (NHL-4U), 6610i (RM-37), 6620 (NHL-12), 6650 (NHM-1), 6800 (NHL-6), 6800A (NSB-9), 6810 (RM-2), 6820A (NHL-9), 6820B (RH-26), 6822 (RM-69), 7200 (RH-23), 7210 (NHL-4), 7250 (NHL-4J), 7250i (NHL-4JX), 7260 (RM-17), 7270 (RM-8), 7280 (RM-14), 7600 (NMM-3), 7710 (RM-12), 8270 (NSD-5FX), 8280 (RH-10), 8310 (NHM-7), 8390 (NSB-8), 8800 (RM-13), 8910 (NHM-4), 8910i (NHM-4NX), 9300 (RAE-6), 9500 (RA-2), D211 (DTE-1)
DCT-L	9290 (RAB-3), 9210 (RAE-3), 9210I (RAE-5)
WD-2	N-GAGE (NEM-4), 3600/3620 (NHM-10), 3650/3660 (NHL-8), 7650 (NHL-2NA), 6600 (NHL-10), N-GAGE QD (RH-29, N-GAGE QDA (RH-47), 7610 (RH-51), 7610B (RH-52), 6670 (RH-67), 6670B (RH-68), 6260 (RM-25), 3230 (RM-51)

деленные затруднения. Например, очень долгое время считалось, что в телефонах NOKIA невозможно менять IMEI-номер. Это было вызвано тем, что CPU, COBBA и FLASH содержат в так называемой OTP-зоне (программируемая однократно в заводских условиях) определенные данные, а в EEPROM на их основе записывается некая результирующая контрольная сумма. При попытке смены IMEI или при замене одной из микросхем при ремонте аппарата (например, при замене микросхемы COBBA) эта контрольная сумма уже не будет соответствовать исходной, поэтому аппарат блокировался сразу в 4 вида блокировки (lock) и разблокировать его было практически невозможно. Более обобщенно можно сказать, что микросхемы CPU, COBBA и FLASH определенным образом взаимосвязаны (в смысле системы защиты), а результирующий код (данные) этой конфигурации хранится в OTP-области памяти, и поэтому любое нарушение этого соответствия (смена IMEI, замена одной из этих микросхем, различные операции с EEPROM и др.) может привести к блокировке аппарата. В настоящее время, с появлением новых сервисных программ, эта проблема успешно решена (подробнее на этих программах мы остановимся ниже).

Отличительной особенностью телефонов NOKIA является отсутствие выведенного на корпус аппарата сервисного соединителя. Он, как правило, находится на основной электронной плате под аккумулятором телефона. В аппаратах NOKIA имеются 2 типа внешних интерфейса: F-bus (имеет две раздельные линии приема/передачи — RX/TX) и M-bus (имеет одну линию приема/передачи). В некоторых случаях (например, при программировании FLASH-памяти телефона) используются оба типа. При этом по шине M-bus телефон управляется на командном уровне, а по шине F-bus происходит обмен с памятью аппарата (в том числе и прошивка). По шине M-bus также выполняют отдельные операции, не требующие больших объемов передачи/приема данных: при смене IMEI-номера, снятии блокировок, получении справочной информации (например, при отображении серийного номера микросхемы COBBA) и др.

Телефоны на платформе DCT-4 уже выполнены совсем на другой элементной базе: в ней, например, уже используется отдельная микросхема UEM, одной из функций которой является обеспечение функционирования системы защиты (от смены IMEI-номера, от вмешательства в изменение содержимого ПО телефона и др.). В этой микросхеме также реализованы контроллер питания и зарядки АКБ, звуковой тракт и узел сигнального процессора (DSP) COBBA. Микросхема FLASH-памяти выполнена в отдельном корпусе. Телефоны 6510 и 8310 являются показательными для этой платформы: их система управления выполнена на трех микросхемах — CPU, UEM (в ней расположена OTP-область) и FLASH. На данный момент считается, что, например, смена IMEI-номера в аппаратах на платформе DCT-4 (и на всех более поздних версиях платформ — см. выше) невозможна без установки новой микросхемы UEM с чистой OTP-зоной. Использование оригинальных заводских управляющих программ, соответствующего сервисного оборудования и заводской поддержки (через сервер NOKIA) — позволяет лишь восстановить исходный IMEI-номер (в случае повреждения содержимого EEPROM при нажатии на клавиатуре комбинации *#06#, вместо IMEI отображаются «**??????????????**» или «**?????????????4**» — это означает, что аппарат заблокирован (в четырех видах блокировки — 4 lock)). При этом, возможна замена содержимого FLASH-памяти аппарата (ПО, языковые пакеты и др.).

Примечание. *Наиболее «продеинутым» ремонтникам удается менять IMEI-номер. На сегодняшний день существует деа способа смены IMEI. В первом случае заменяют микросхему UEM на новую (с чистой OTP-зоной) и программируют эту зону специальным RPL-файлом содержащим некий «чужой» IMEI-номер. Но для этого необходимы определенные навыки и соответствующее оборудование.*

Во втором случае используется специальный бокс, позволяющий «патчить» (или модифицировать) содержимое FLASH-памяти телефона на предмет проверки IMEI в OTP-зоне, что позволяет таким образом менять IMEI-номер на совершенно произвольный, заданный вручную. К сожалению, это оборудование только недавно появилось на рынке и является «сырым». На данный момент поддерживаются не все модели телефонов и не все версии ПО, и самое главное— нет возможности восстановления IMEI, если повреждены данные в EEPROM (в этом случае IMEI-номер на экране телефона выглядит как «??????????????»).

Для платформ DCT-1 — DCT-3 компанией NOKIA использовался программный пакет, называемый WinTesla. Телефоны подключают к LPT- и COM-портам ПК (через соответствующие адаптеры интерфейсов F-bus и M-bus — см. выше) и с помощью специального электронного ключа «прошивают» ПО телефона, калибруют радиотракт и др.

Для платформы DCT-4 (и всех последующих) NOKIA выпустила более защищенное программное обеспечение, именуемое PHOENIX. Оно работает со специальными боксами, служащими дополнительным ключом защиты этой программы. Подобное программное и аппаратное обеспечение поставляется только в авторизованные центры NOKIA. А всем остальным приходится довольствоваться устройствами, которые функ-

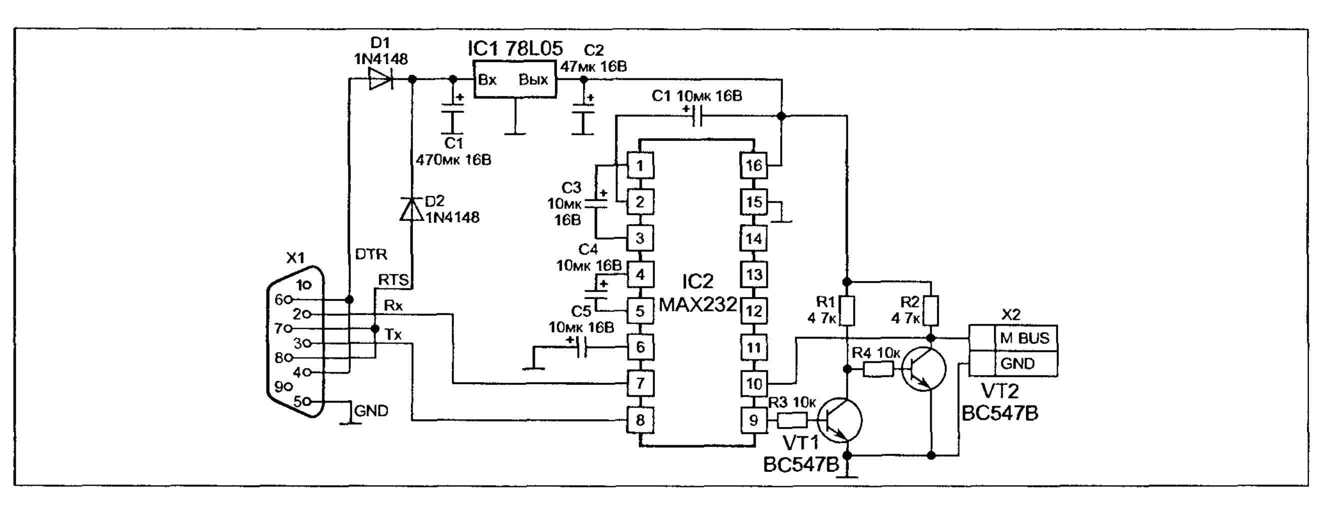


Рис. 8 1 Кабель M-BUS

ционально эмулируют заводское программное обеспечение

Следует отметить, что у компании NOKIA, кроме коммерческих названий аппаратов, существуют также и сервисные названия (см табл 8 1) — например, модель «Nokia 5110» (коммерческое название), выполненная на платформе DCT-3, имеет сервисное название NSE-1 А смартфон «Nokia 7650» (платформа WD2) имеет сервисное «имя» NHL-2NA Сервисное название необходимо, так как тем же именем обозначаются имена файлов прошивок, названия кабелей-переходников и др Соответствие сервисных и коммерческих названий телефонов можно найти в меню программ прошивки, речь о которых пойдет ниже

Для программирования телефонов, выполненных на платформах DCT-3, DCT-4, а также более поздних, например, WD2, необходимо иметь специальные боксы и кабели-переходники

Схема простейшего из них — кабеля M-bus (для DCT-3) приведена на рис 8 1, а схема для программирования FLASH-памяти через интерфейс F-bus для этой же платформы — на рис 8 2 Второй кабель предполагает подключение к LPT-порту ПК, в настройках этого порта необходимо установить режимы ESP/EPP или BI-DIRECTIONAL

Конечно, для программирования телефонов лучше всего использовать универсальные боксы, предназначенные для одной или нескольких платформ, например, наиболее распространенные из них — UFS (Twister) и Griffin Внешний вид этих боксов показан, на рис 8 3 (UFS — сверху, а Griffin — внизу), а принципиальные схемы — соответственно, на рис 8 4 и 8 5

Во всех случаях на ПК желательно использовать ОС Windows 98 SE, за исключением работы с боксом UFS, так как он использует интерфейс

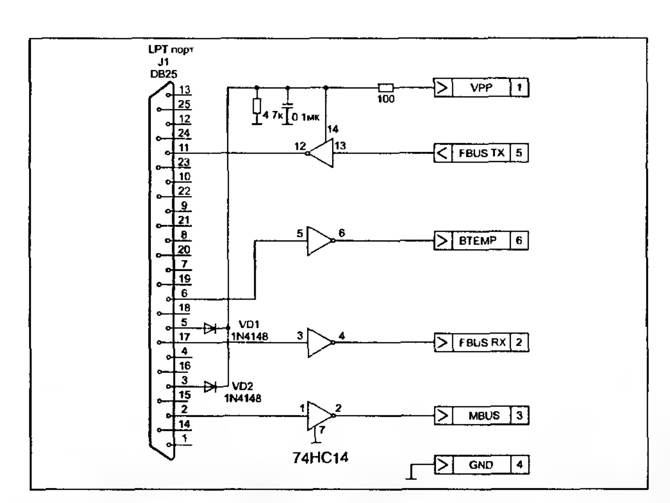


Рис. 8.2 Кабель F-BUS

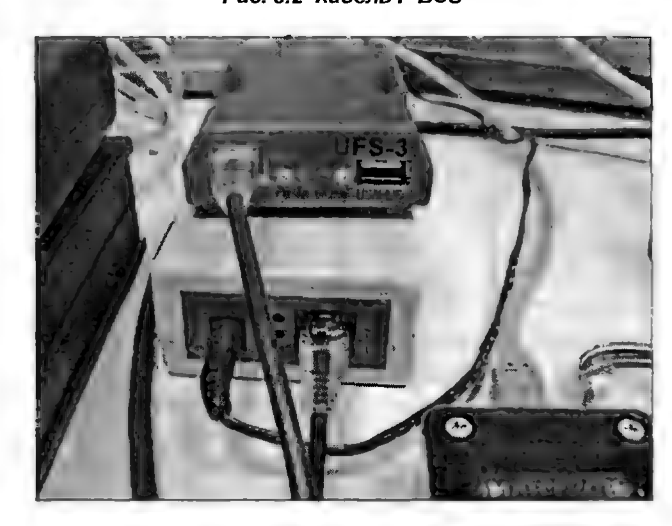


Рис. 8.3. Боксы UFS и GRIFFIN

USB — и в этом случае лучше пользоваться Windows XP

Также следует отметить достаточно распространенный (и дешевый) так называемый «чип-флешер», предназначенный для программирования телефонов NOKIA на платформе

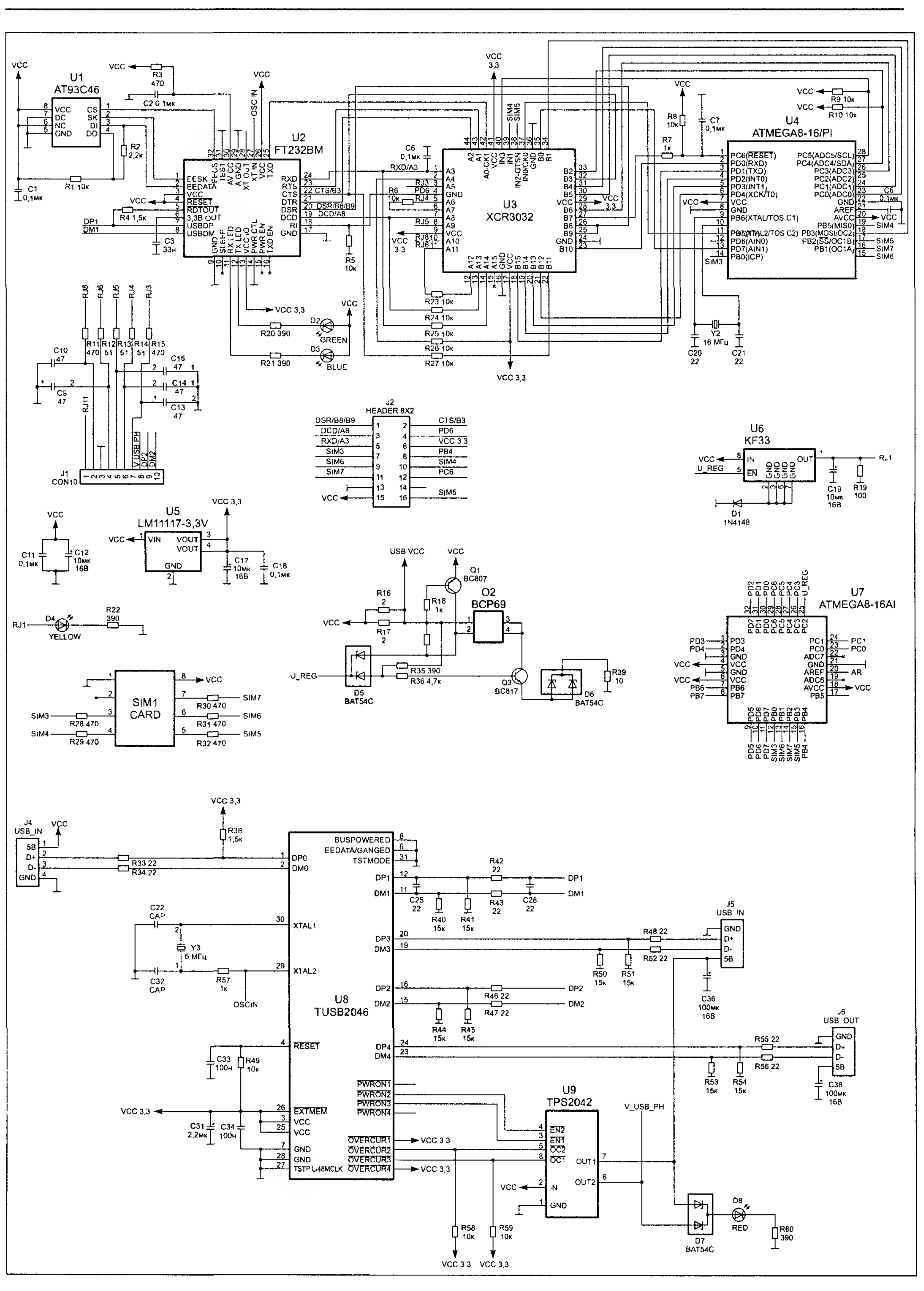


Рис. 8.4. Принципиальная схема бокса UFS

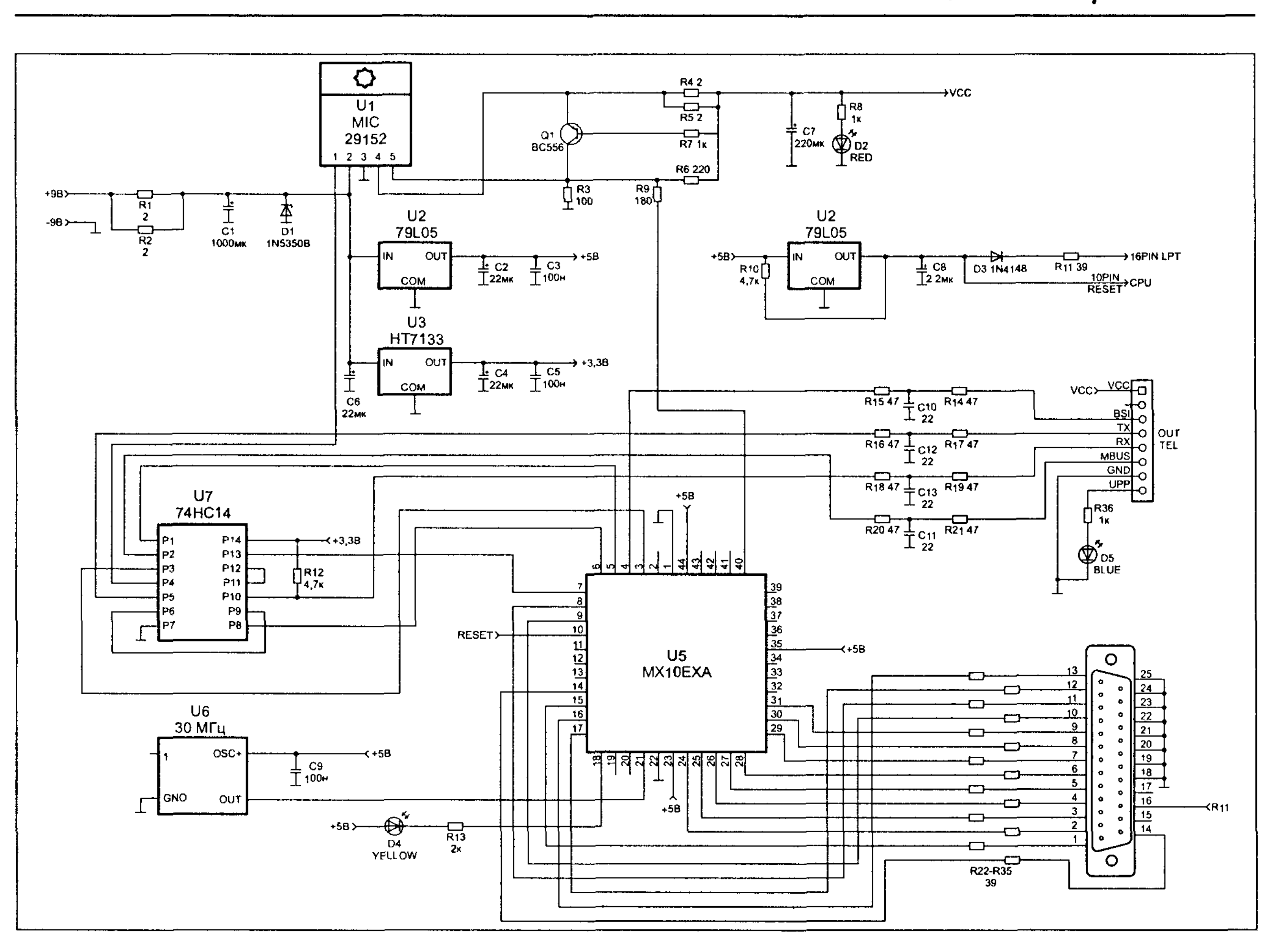


Рис. 8.5. Принципиальная схема бокса GRIFFIN

DCT-4 (около 10 моделей) и выполненный на PIC-контроллере типа 16F877.

На рынке существует масса программ для программирования телефонов NOKIA, они отличаются «привязкой» к конкретному типу бокса, интерфейсами (M-bus, F-bus или универсальный), а также другими функциональными возможностями.

Остановимся на наиболее популярных из них.

Программирование телефонов, выполненных на платформе DCT-3

Одна из наиболее популярных программ для аппаратов, выполненных на платформе DCT-3 — это NokiaTool. С ее помощью можно считывать коды блокировки, произвести программный сброс телефона на заводские установки, включать дополнительные модификации и др.

Для ее функционирования необходим адаптер COM-порт/M-bus (рис. 8.1) или универсальный бокс (см. выше).

Окно программы Nokia Tool (версии 5.01) показано на рис. 8.6.

Примечание. *Перед тем, как начать работу с этой программой, подключают адаптер через переходник к телефону, а затем уже включают телефон.*

Нажимают кнопку READ PH (1 на рис. 8.6), и в ранее пустых окнах программы появится информация о версии ПО телефона, типе аппарата, дате его изготовления, IMEI-номерах (в EEPROM и FLASH), коде телефона (заводская установка кода — 12345), состоянии блокировок.

Установив в окне FACTORY SETTING (2 на рис. 8.6) необходимые опции и нажав кнопку 3 APPLY FS можно сбросить настройки телефона на заводские, счетчики и др.

Кнопкой 4 SW RESET устанавливаются все опции окна 2 на заводские, в этом случае код блокировки телефона будет 12345.

Ремонтники, как правило, используют эту программу только для определения кода блокировки телефона (SECURITY CODE в окне INFO на рис. 8.6).

Остальные опции программы NokiaTool используются достаточно редко, поэтому подробно останавливаться на них не будем.

Примечание. *Телефоны NOKIA после трех неудачных попыток разблокировки аппарата перестают принимать даже правильный код (который*

был определен с помощью программы Nokia-Tool) Выходят из этой ситуации следующим образом оставляют включенный телефон с запросом ввода кода разблокировки в течение пяти минут После этого код вводят еще раз, и в большинстве своем повторных попыток уже не требуется

Следующая популярная программа для работы с телефонами NOKIA — это Nokia Tool от Rolis, ее окно показано на рис. 8.7.

Этот пакет по сравнению с предыдущим более функционален и позволяет:

- изменять IMEI-номер телефона. Для этого меняют содержимое окна 1 (рис. 8.7) и нажимают кнопку 2 CHANGE. При этом оригинальный IMEI-номер в окне 3 может быть другим. Это, как правило, не сказывается на работоспособности телефона;
- восстановить оригинальный IMEI-номер, для этого в окне 1 вводят номер, считанный из окна 3 и нажимают кнопку CHANGE;
- проверить версию сигнального процессора DSP, входящего в состав микросхемы COBBA — см. окно 4);
- проверить версию языкового пакета (Lg) в окне 5, и в ниспадающем меню 6 выбрать языки, входящие в этот языковой пакет;
- менять значение контрастности дисплея регулятором 7;
- в модели 3310 (с помощью кнопок 8) можно активировать/деактивировать дополнительные пункты пользовательского меню;
- проверить серийный номер микросхемы COBBA (окно 9), контрольные суммы языкового пакета CHK (окно 10) и файла сигнатуры (окно 11) и др.

Следует отметить, что если указанные контрольные суммы и номер COBBA ID неправильные, то в аппарате включаются четыре вида бло-

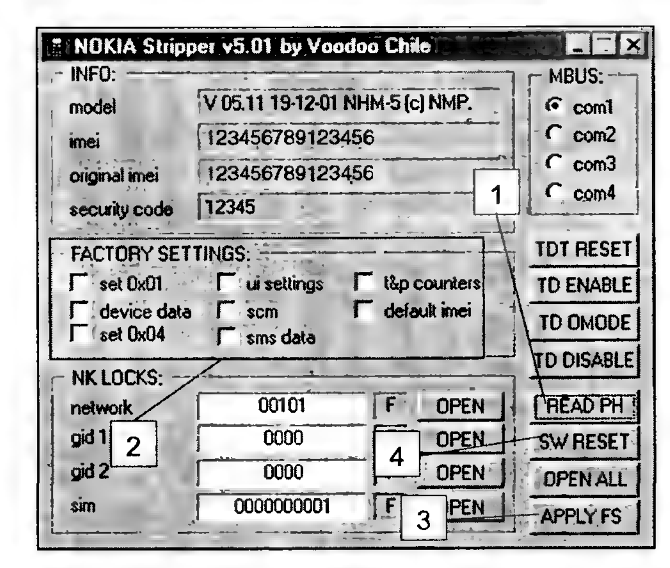


Рис. 8.6

кировки (4 lock). Это происходит, например, при замене микросхемы COBBA. Общую контрольную сумму на основе этих кодов еще называют MSId — ее можно корректировать, нажав кнопку FAID (12).

В случае блокировки 4 lock (а также, если аппарат заблокирован на оператора), и когда в окне 9 (рис. 8.7), все нули — это указывает на физическую неисправность микросхемы COBBA. В этом случае на экране телефона отображается сообщение «ВСТАВЬТЕ ПРАВИЛЬНУЮ КАРТУ» (или «SIM НЕ ПОДХОДИТ»).

Закладка 13 — NET MONITOR (СЕТЕВОЙ МОНИТОР) позволяет включать этот режим, сбрасывать его в исходное состояние, а также с помощью него снимать служебную информацию об операторе, базовой станции (мощность станции, удаление до нее, цифровой код оператора и др.).

Закладки READ и WRITE (14 и 15) позволяют читать и записывать содержимое Flash-памяти телефона.

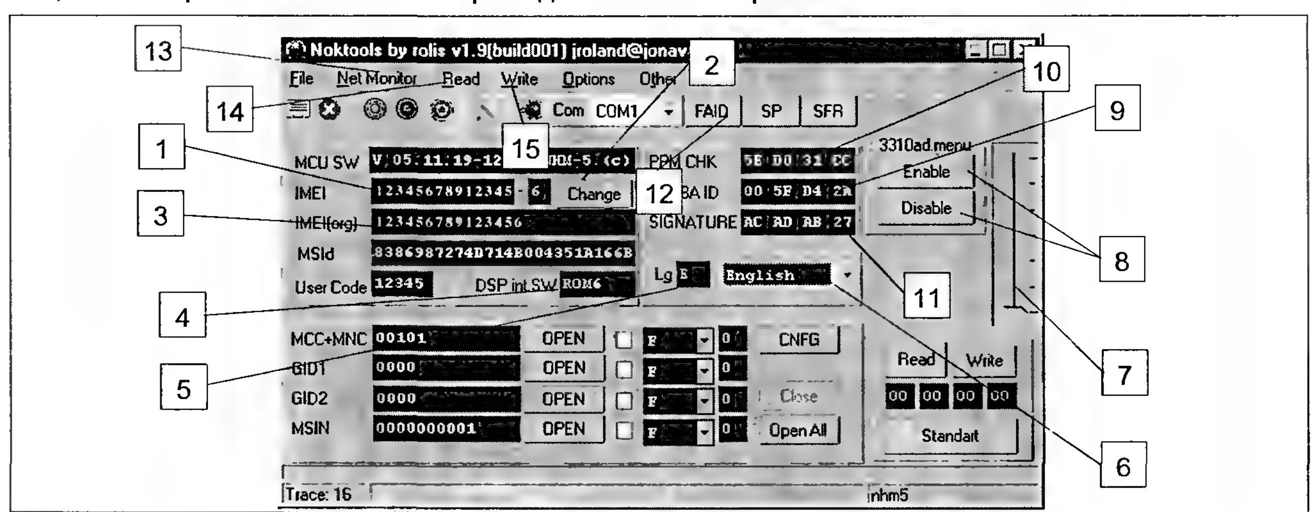


Рис. 8.7

Рис. 8.8

Следующий пакет с аналогичным названием — Nokia Tool, но от другого производителя @Bullet- = Jordik. Его окно показано на рис. 8.8 Он используется для снятия блокировок, замены IMEI-кодов и сброса телефона на заводские установки.

Эта программа по своим функциональным возможностям аналогична предыдущей, поэтому подробно на ней мы останавливаться не будем.

Теперь рассмотрим очень простую и полезную программу, называемую EEPROM TOOL, ее окно показано на рис 8.9.

Эта программа позволяет.

— менять (восстанавливать) IMEI-номер;
— считывать различную справочную информацию;
— производить сброс аппарата на заводские установки Подобная операция позволяет восстанавливать аппараты, у которых появились проблемы с сетью (например, если появляется полная шкала сети, а затем она пропадает) При сбросе настроек телефона восстанавливается содержимое EEPROM, в которых записаны и настройки радиоканала;
— тестировать микросхему COBBA.

Программа EEPROM TOOL является идеальным инструментом для разблокировки телефонов (если, конечно, аппарат не находится в состоянии CONTACT SERVICE) Например, если в телефоне была полностью перезаписана Flash-память — он, естественно, будет заблокирован (4 lock) и у него будет неправильный IMEI-номер. С помощью этой программы можно

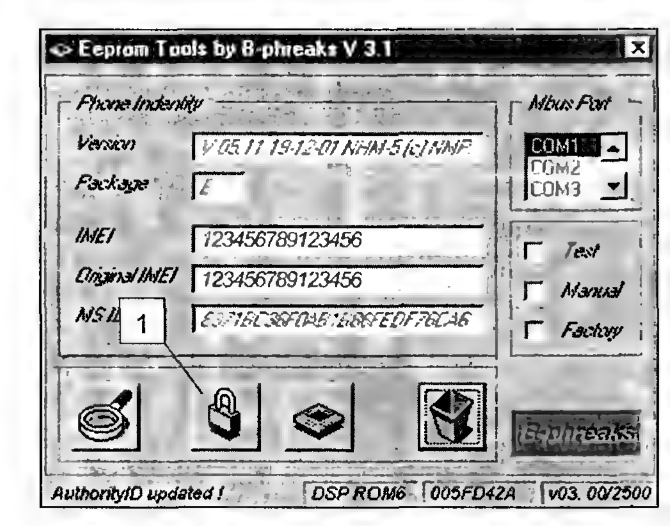


Рис. 8.9

быстро выполнить разблокировку аппарата (кнопкой 1), а затем восстановить IMEI-номер.

Если же в аппарате невозможно выполнить указанные операции, используют ранее рассмотренные программы

Примечание. *Для всех телефонах NOKIA приняты следующие сокращения расширений файлов прошивки*

- *MCU— основное ПО,*
- *PPM — языковой пакет,*
- *CNT — область CONTENT (картинки, мелодии и др),*
- *PM — файл, содержащий настройки радиоканала (эти файлы применимы для платформы DCT-4 и всех последующих),*
- *PMM — файл прошивки EEPROM*
- *RPL — файлы, предназначенные для записи IMEI-кодое в «чистые» микросхемы UEM (для платформы DCT-4)*

Для прошивки ПО телефонов на платформе DCT-3 необходим универсальный бокс, имеющий интерфейс F-bus, а также соответствующее программное обеспечение (или так называемый «флешер»). В простейшем случае можно воспользоваться DATA-кабелем F-bus, показанным на рис. 8.2.

Рассмотрим подробнее порядок прошивки ПО телефона.

Выключенный телефон подключают к кабелю F-bus и на ПК запускают программу — в нашем случае мы остановимся на Nokia DCT-3 flasher by Rollis. Окно программы показано на рис. 8.10. Эту программу еще называют БАНАН — это связано с тем, что в качестве иконки (слева вверху) показан фрукт с аналогичным названием.

Программа Nokia DCT-3 flasher позволяет:

- считывать и записывать различные области Flash-памяти телефона (в том числе и выборочно);
- разблокировать и заблокировать телефон;
- проверить и пересчитать контрольные суммы (см. выше);
- проверить и при необходимости исправить считанный FLASH-файл на предмет возможных ошибок (с помощью опции SCAN FLASH). Если в телефоне запорчен Flash-файл (ПО), на экране дисплея высветится сообщение CONTACT SERVICE;
- можно отдельно загрузить различные файлы, например — PPM, MCU и др. После этого необходимо скорректировать контрольные суммы аппарата. Последнюю операцию необходимо проводить обязательно, так как в противном случае аппарат заблокируется (4 lock) или перейдет в состояние CONTACT SERVICE.

В окне 1 этой программы выбирают модель аппарата (в скобках дано его сервисное название). Затем выбирают файл «прошивки», область памяти и затем, собственно, записывают этот файл в телефон. С помощью этого пакета можно записать как оригинальную (что была ранее), так и более позднюю версию ПО телефона.

Существуют программы-флешеры, которые объединяют работу интерфейсов M-bus, F-bus. Один из них — **Nokia DCT3 flasher&m2bus tools** от компании Rollis. Окно этой программы показано на рис. 8.11.

Эта программа имеет много функциональных возможностей (в большинстве своем мы на них останавливались), перечислим некоторые из них:

- конвертация оригинальных файлов «прошивок» NOKIA (предназначенных для пакета WinTesla) в бинарный формат (который «понимают» другие программы-флешеры);
- перепрограммирование телефона «Nokia 3310» в «Nokia 3315»;
- чтение и прошивка MCU, PPM, EEPROM;
- чтение справочной информации о телефоне (рис. 8.11). Подобная информация аналогична той, которую можно получить с помощью уже рассмотренных выше программ;
- совмещает в себе все функции программы-флешера (через интерфейс F-bus) и Nokia Tool (работающего через M-bus) от Rollis. Например, с помощью опции 1 Flash (рис. 8.11) можно производить флеширование аппарата, а Read m2bus (2) и Write m2bus (3) — операции разблокировки, чтения служебной информации и др.

Есть еще одна программа, предназначенная для прошивки FLASH-памяти телефона. Она называется DEJAN FLASHER, выполняет те же функции, что и Nokia DCT-3 flasher, поэтому по-

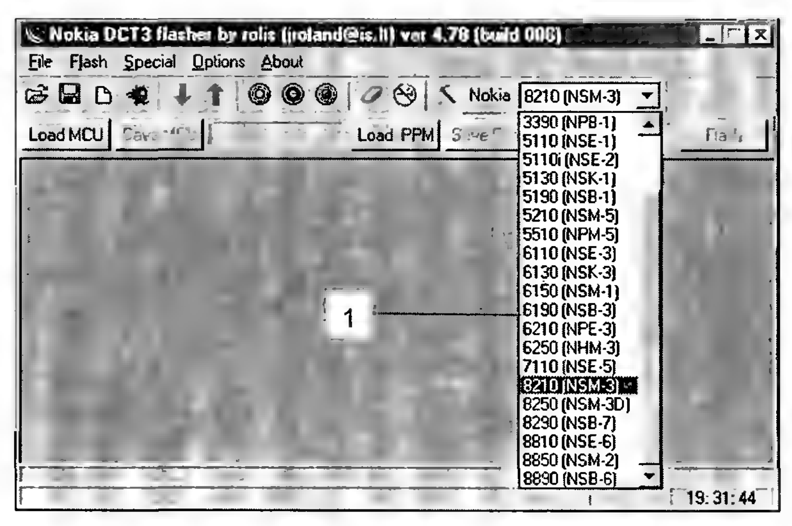


Рис. 8.10

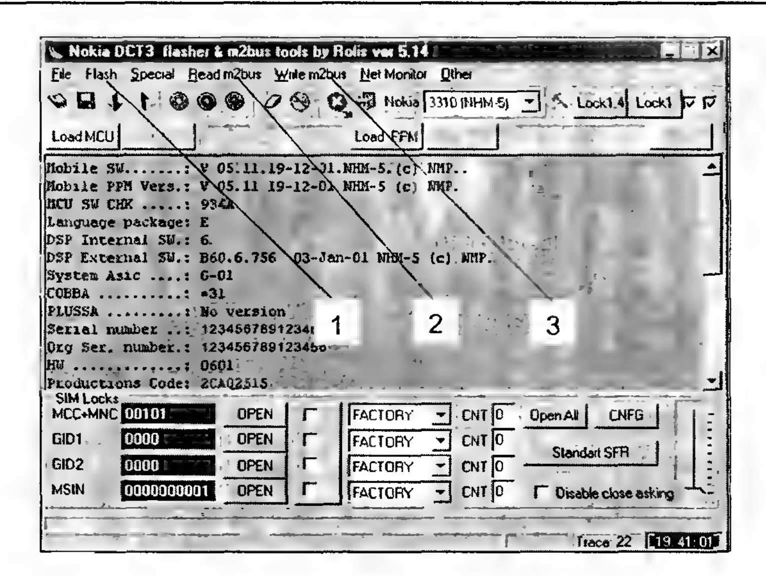


Рис. 8.11

дробно останавливаться на ней мы не будем. Отметим лишь, что существует две версии этой программы FULL и LIGHT — их возможности понятны из названия.

Программирование телефонов, выполненных на платформе DCT-4

Для программирования телефонов DCT-4 удобнее всего использовать стандартные боксы GRIFFIN или UFS. Их особенностью является то, что они «понимают» стандартные фирменные пакеты для «прошивки» телефонов NOKIA всех серий. Достаточно инсталлировать пакет с прошивкой и пользоваться этим программным обеспечением исходя из его функциональных возможностей (не нужно конвертировать файлы из одного формата в другой и выполнять другие лишние действия).

Как уже отмечалось, аппараты на платформе DCT-4 имеют мощную систему защиты, в них, например, нельзя полностью считать содержимое Flash-памяти, а лишь только определенные (разрешенные) области.

Остановимся подробнее на программировании телефонов с помощью бокса GRIFFIN.

Программирование телефонов на платформе DCT-4 с помощью универсального бокса GRIFFIN

Окно программы **Griffin v2.087** показано на рис. 8.12.

С помощью бокса GRIFFIN на телефонах платформы DCT-4 можно выполнять следующие операции:

— полностью перепрограммировать аппарат: менять содержимое MCU (1 на рис. 8.12), PPM (2), CONTENT (SP File (3)), а также программировать на некоторых моделях режимы DSP (ADSP (4)). При прошивке телефона следует учесть, что версия ПО языкового пакета PPM должна соответствовать версии MCU;

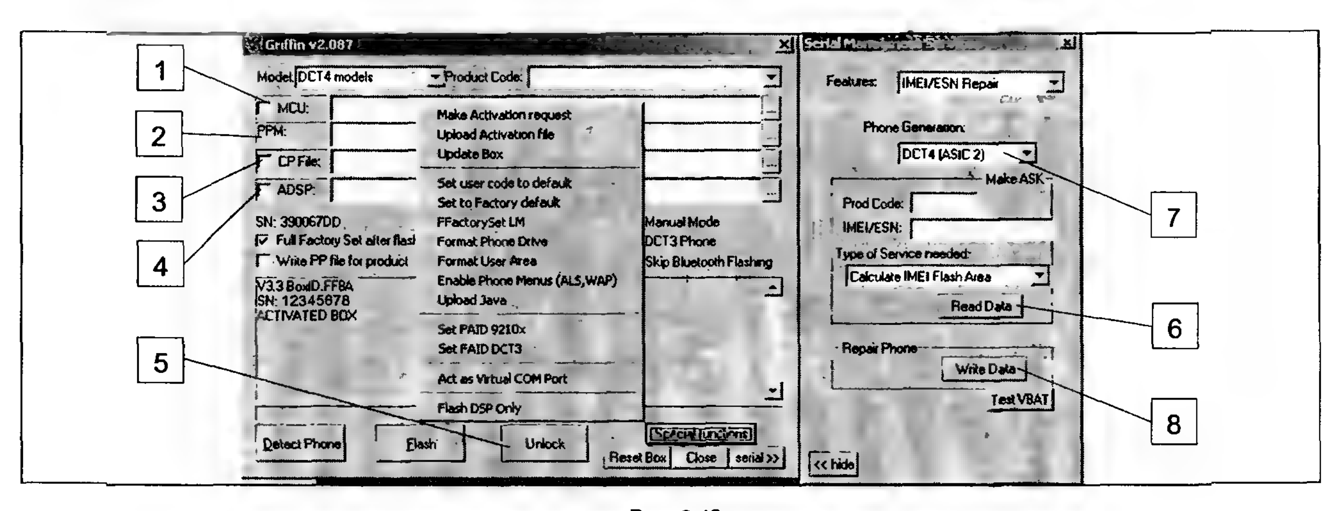


Рис. 8.12

— производить сброс аппарата на заводские установки (сброс пользовательского кода на код по умолчанию, а также полный и выборочный сброс);
— производить форматирование в последних моделях телефонов так называемого виртуального диска;
— блокировку/разблокировку аппарата. Кнопка 5 Unlock используется только для снятия операторской блокировки, пользовательские блокировки снимаются сбросом аппарата на заводские установки (активируют опцию FFactory-Set LM), при этом код телефона принимает значение 12345 (по умолчанию);
— форматировать пользовательскую память (CONTENT);
— активировать новые пункты пользовательского меню;
— загружать JAVA-приложения;
— добавлять и при необходимости удалять пользовательские функции (меню) аппарата;
— считать/записать код продукта. Это очень важная функция, необходимая при восстановлении IMEI-номера, решения проблем, вызванных состоянием аппарата CONTACT SERVICE;
— менять и восстанавливать настройки радиоканала (PM-файл). Часто эта функция позволяет восстановить работоспособность радиоканала (некоторые ремонтники в подобных случаях «грешат» на аппаратное обеспечение).

Естественно, с появлением новых моделей телефонов, для работы с ними необходимы обновления программного обеспечения и прошивки самого бокса GRIFFIN. Это можно сделать с сайта поддержки www.griffin.com.

Окно программы Griffin (рис. 8.12) разделено на две половины: левая часть предназначена для «флеширования» телефона, а правая — для дополнительных функций. Например, одна из примечательных дополнительных функций — тестирование телефона. Допустим, если аппарат находится в состоянии CONTACT SERVICE, причину данного состояния и выявляет данная программа (DSP, проблемы с блокировкой и др.).

Рассмотрим возможные неисправности телефонов на платформе DCT-4 и способы их устранения с помощью пакета Griffin.

Телефон переходит в состояние CONTACT SERVICE, а указанный выше тест показывает наличие в аппарате операторской блокировки

Для устранения подобного дефекта достаточно нажать кнопку UNLOCK (5 на рис. 8.12).

В смартфонах (платформа WD-2) часто проявляется дефект, когда они «зависают» в момент появления на экране картинки приветствия

В подобном случае форматируют пользовательскую память аппарата (USER AREA), а затем выполняют его полный сброс командой сброса, введя на включенном телефоне комбинацию *#7370#, а затем — код телефона 12345 (FULL FACTORY SET).

Иногда при неправильном программировании телефона (*#06#) вместо IMEI-кода появляются вопросительные знаки, одновременно аппарат блокируется. То же самое бывает, если меняется отдельно одна из микросхем — UEM или FLASH (из другого аппарата)

Уже ранее отмечалось, что в аппаратах на платформе DCT-4 (и более поздних) используется развитая система защиты на основе упомянутых микросхем, поэтому замена одной из них активирует эту защиту. Выходят из подобной ситуации, заменяя эти микросхемы парно (например, выпаяв обе из «донорского» аппарата).

Восстановить оригинальный IMEI-номер можно несколькими способами.

1. Подключают телефон к GRIFFIN и нажимают кнопку READ DATA (6 на рис. 8.12), но перед этим необходимо правильно выбрать версию ASIC (7) — или поколение микросхем UEM. После этого вводят оригинальный серийный номер аппарата (он нанесен на наклейке, под задней крышкой телефона). После чего программа формирует так называемый файл запроса (ASK-файл). Этот файл передают (за определенную плату — около 8 евро) реселлеру(ам) (будем называть их так), которые пересылают его через Интернет его на головной сервер NOKIA, а в ответ получат специальный RPL-файл с исправленными контрольными суммами для этой модели аппарата. Полученный файл записывают в телефон, нажав кнопку 8 WRITE DATA. В итоге в аппарате мы получим восстановленный исходный IMEI-номер.
2. Приобретают «чистую» микросхему UEM, впаивают ее в телефон и программируют аппарат так называемым «патченным» RPL-файлом. Что же касается IMEI-номера, хранящегося в EEPROM, то RPL-файл изменяет его таким образом, что он будет совпадать с номером, расположенным в UEM.

Отметим, что «патченные» RPL-файлы кроме своей основной функции («прошивки» UEM) модифицированы таким образом, что они меняют

EEPROM в соответствии с приведенным выше алгоритмом (оригинальные RPL-файлы такой особенностью не обладают).

Программирование телефонов с помощью универсального бокса UFS

С помощью универсального бокса UFS можно программировать телефоны, выполненные не только на платформах DCT-3, DCT-4, но и DCT-L и WD-2.

Программная оболочка этих боксов называется DCTx Tools, ее окно показано на рис. 8.13 (в закладке выбрана платформа DCT-3).

Приставка к названию этой программы — SarasSoft (см. рис. 8.13) означает имя производителя, а Saras — это один из разработчиков, в свое время работавших на разработке программного обеспечения боксов GRIFFIN. Этот экскурс необходим нам для того, чтобы знать, что в программе DCTx Tools используется много наработок от программы GRIFFIN — это своего рода программа-преемник последней, но с более широкими возможностями.

Программа DCTx Tools в первую очередь удобна тем, что она поддерживает максимально возможный набор функций, необходимых для работы с телефонами NOKIA. Кроме того, она является достаточно гибким инструментом хотя бы из-за того, что поддерживает режим сценарной обработки (то есть можно самостоятельно запрограммировать цепочку выполнения определенных операций).

В этой программе есть развитая система понятных подсказок, кроме того, существует подробная инструкция для работы с ней. Поэтому, перед тем, как приступать к программированию конкретной модели телефона, необходимо ознакомиться с соответствующим разделом инструкции, в противном случае это может привести к плачевным последствиям. Например, с помощью этой программы в смартфонах (платформа WD-2) нельзя проводить полный сброс, в противном случае аппарат перейдет в состояние CONTACT SERVICE.

Кроме того, программа DCTx Tools позволяет:

— выбирать тип интерфейса (M-bus, F-bus);
— работать с компьютером через интерфейс USB;
— поддерживать практически все аппараты NOKIA (в этой программе записаны адреса — — расположения различных областей памяти, поэтому их программирование может происходить автоматически — адреса вводятся вручную при «тонкой» настройке аппарата);
— проверять работоспособность процессорной части телефона (с помощью кнопки 1 CHECK — см. рис. 8.13). Если точнее, основное назначение этой функции — проверка соединения с аппаратом посредством загрузки в процессор телефона специальной программы-загрузчика. Для ремонтников это должно быть важно — если операция после нажатия кнопки CHECK прошла успешно — на телефоне можно проводить операции чтения/записи Flash-памяти;
— перезаписывать область EEPROM и менять IMEI-номер. Правда, при записи EEPROM в телефон DCT3 иногда необходимо преобразовать файл EEPROM в формат, понятный UFS, для этого исходный FLS-файл переиме-

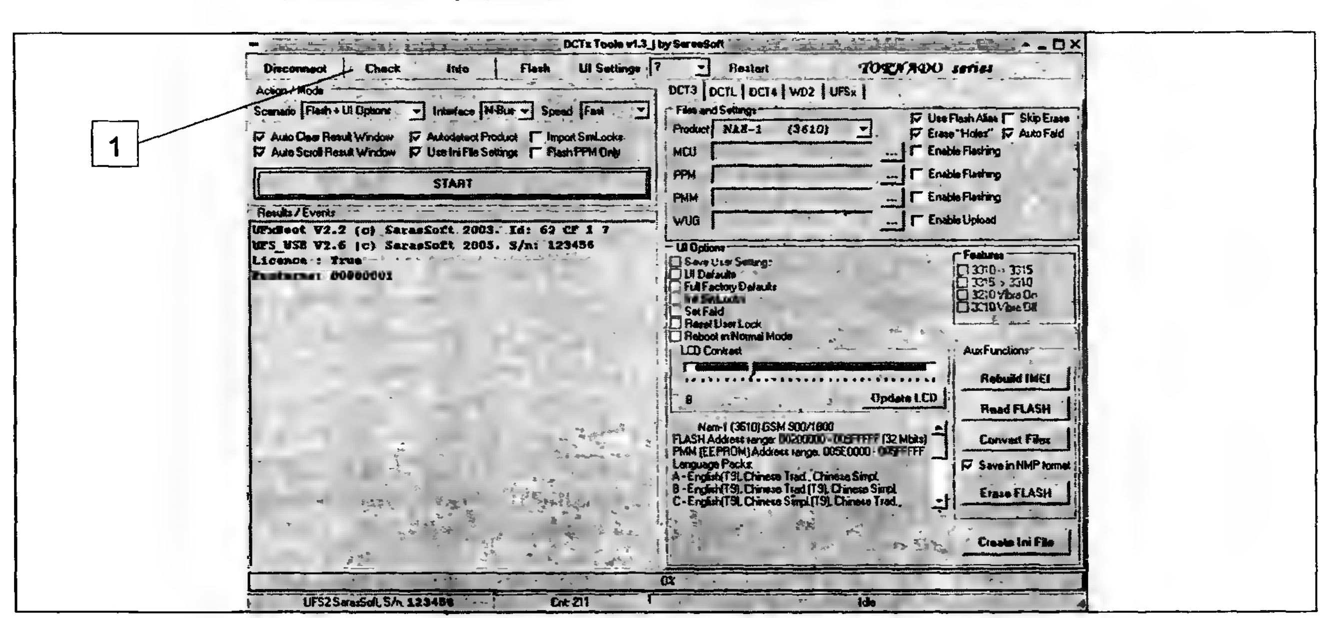


Рис. 8.13

новывают в формат BIN и, нажав кнопку CONVERT, выбирают этот файл. После этого программа запросит область адресов, в которую файл должен быть записан. Вводят необходимые данные и подтверждают ввод кнопкой OK. После чего этот файл автоматически преобразуется в понятный для программы формат. Открывают этот файл и записывают его в память телефона. После этого выбирают опцию восстановления IMEI-номера, вводят новый (или старый) IMEI меняют и производят сброс телефона на заводские установки.

Перечисление всех возможностей программы займет достаточно много времени, остановимся лишь на наиболее показательных режимах.

Если нажать кнопку INFO и выбрать платформу телефона, можно считать всю техническую информацию об этой модели (как в программных продуктах, описанных выше). После этого, если мы заходим в окно прошивки MCU (или других), программа автоматически выводит нужную директорию с предустановленной прошивкой — остается только подтвердить выбор. Считывание информации возможно, только если телефон включается.

В простейшем случае «прошивку» телефона выполняют следующим образом:

— присоединяют аппарат к боксу UFS и включают телефон;
— выбирают соответствующие друг другу версии MCU и PPM (если необходимо перезаписать только один из указанных компонентов, то соответствие версий также необходимо соблюдать);
— производят необходимые настройки пользовательского интерфейса (UI Setting) и нажимают кнопку START.

Если необходимо узнать версию ПО аппарата, включают его и набирают комбинацию *#0000# , или нажимают кнопку Info в окне программы DCTx Tools. В случае, если телефон не включается, выбирают MCU и PPM, снимают галочку в позиции Autodetect Product и нажимают OK.

На рис. 8.14 показано окно программы для платформы телефонов DCT-4, где числами отмечены некоторые функциональные кнопки, панели и окна (их назначение понятно из названия):

1 — окно сообщений программы;
2 — окно пользовательских установок;
3 — режим ручной прошивки;
4 — настройки пользовательского интерфейса;
5 — переключение режимов (Local Mode, Test mode, Normal Mode);
6 — перезагрузка телефона;
7 — выбор платформ;
8 — панель выбора файлов прошивок;
9 — выбор версии Bluetooth. Также можно восстановить работоспособность Bluetooth, нажав кнопку Rp BT (на панели 14);

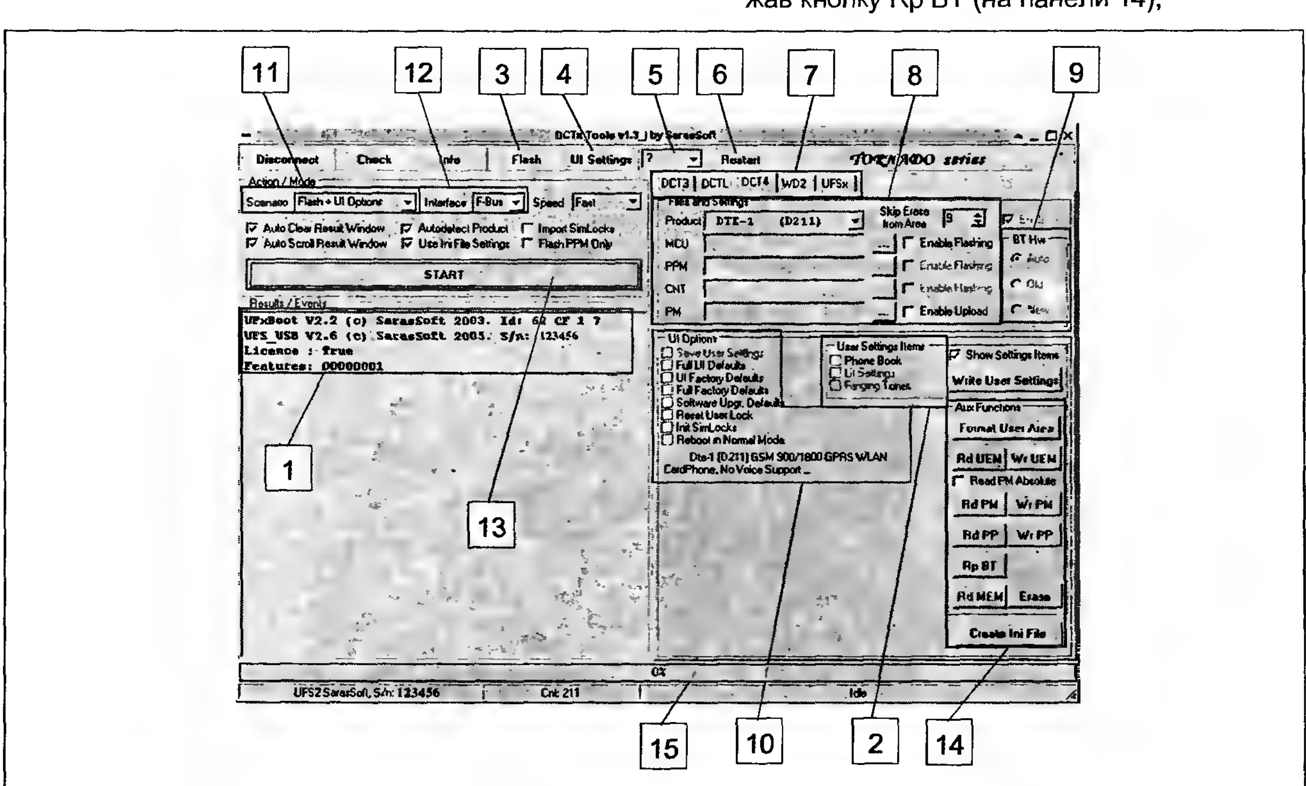


Рис. 8.14

10 — опции настроек режимов программы;

11 — выбор сценария;

12 — выбор интерфейса (M-bus, F-bus);

13 — старт/отмена выбранной операции;

14 — чтение/запись содержимого микросхемы UEM (Rd/Wr UEM — создание ASK-файла и запись RPL-файла), области EEPROM (Rd/Wr PM), чтение всей памяти (Rd MEM), ее очистка (Erase), создание INI-файла (Create Ini File) и другие операции,

15 — прогрессирующая шкала выполнения операций (чтения/записи);

На рис. 8.15 показан процесс ручного выбора модели телефона (в ниспадающем меню 1 для смартфонов на платформе WD-2), а на рис. 8.16 — панель калькуляции кодов разблокировки (1) и панель поддержки программного обеспечения бокса UFS (2).

В заключение приведем еще одну принципиальную схему универсального бокса — см. рис. 8.17.

В табл. 8.2 приведены адреса областей MCU, EEPROM и PPM (в микросхеме Flash-памяти) и русскоязычные версии языкового пакета PPM для некоторых моделей телефонов на платформе DCT3.

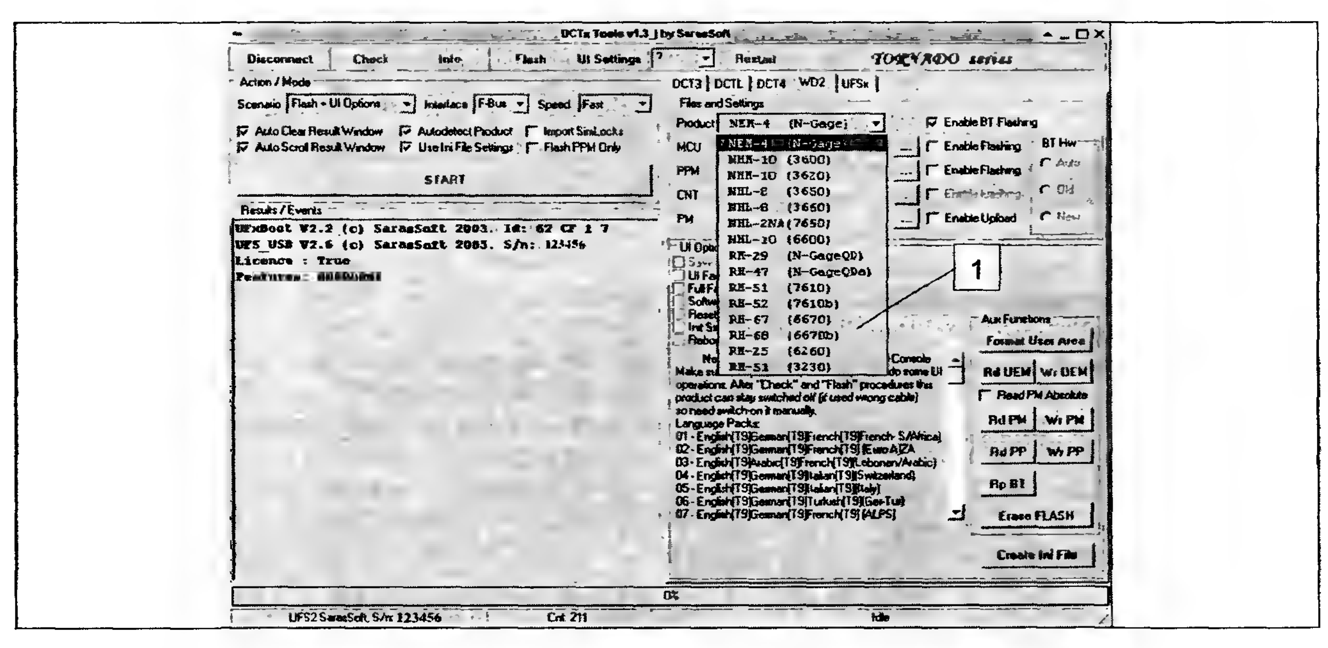


Рис. 8.15

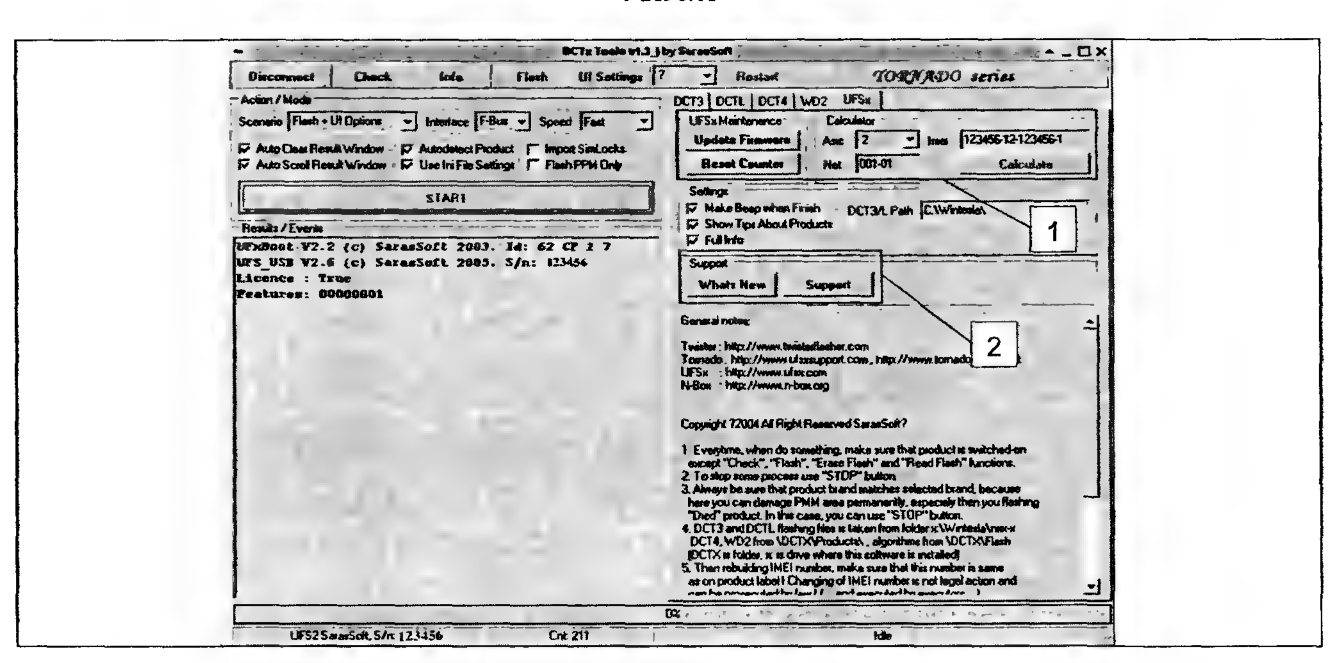


Рис. 8.16

Таблица 8.2

Адресное пространство MCU, EEPROM и PPM в микросхеме FLASH-памяти и версии языкового пакета PPM с русским языком

Модели телефонов NOKIA	Адресное пространство				Версии языкового пакета PPM, имеющие русский язык
	FLASH-память	MCU	PPM	EEPROM	
3210 (NSE-8/9)	00200000-00400000	00200000-002EFFFF	002F0000-003FFFFF	Не содержится в микросхеме Flash-памяти	b
3310, версии ПО – 3.24 и 4.02	00200000-00400000	00200000-0031FFFF	00320000-003CFFFF	003D0000-003FFFFF	e
3310, версия ПО – 04.06 и выше	00200000-00400000	00200000-0032FFFF	00330000-003CFFFF	003D0000-003FFFFF	e
3330, версии ПО – 3.05, 4.12, 4.16	00200000-00600000	00200000-0048FFFF	00490000-0054FFFF	00550000-005FFFFF	d, e, i, j
3330, версия ПО – 3.12	00200000-00600000	00200000-0048FFFF	00490000-005DFFFF	005E0000-005FFFFF	d, e, i, j
3330, версия ПО – 4.30	00200000-00600000	00200000-0048FFFF	00490000-005EFFFF	005F0000-005FFFFF	d, e, i, j
5110 (NSE-1)	00200000-00300000	00200000-002AFFFF	002B0000-002FFFFF	Не содержится в микросхеме Flash-памяти	b
5130 (NSK-1)	00200000-00300000	00200000-002BFFFF	02C00000-002FFFFF	Не содержится в микросхеме Flash-памяти	b
6110 (NSE-3)	00200000-00300000	00200000-002BFFFF	002C0000-002FFFFF	Не содержится в микросхеме Flash-памяти	b
6130 (NSK-3)	00200000-00300000	00200000-002CFFFF	002D0000-002FFFFF	Не содержится в микросхеме Flash-памяти	b
6150 (NSM-1)	00200000-00400000	00200000-0035FFFF	00360000-003FFFFF	Не содержится в микросхеме Flash-памяти	a, g
6210 (NPE-3)	00200000-00600000	00200000-0051FFFF	00520000-0059FFFF	005A0000-005FFFFF	g, i
6250 (NHM-3)	00200000-00600000	00200000-0052FFFF	00530000-0059FFFF	005A0000-005FFFFF	g, i
7110 (NSE-5)	00200000-00600000	00200000-0050FFFF	00510000-0058FFFF	00590000-005FFFFF	b, e
8210 (NSM-3)	00200000-00400000	00200000-0033FFFF	00340000-003CFFFF	003D0000-003FFFFF	d, g
8850 (NSM-2)	00200000-00400000	00200000-0033FFFF	00340000-003CFFFF	003D0000-003FFFFF	d, g
8890 (NSB-6)	00200000-00400000	00200000-0033FFFF	00340000-003CFFFF	003D0000-003FFFFF	d

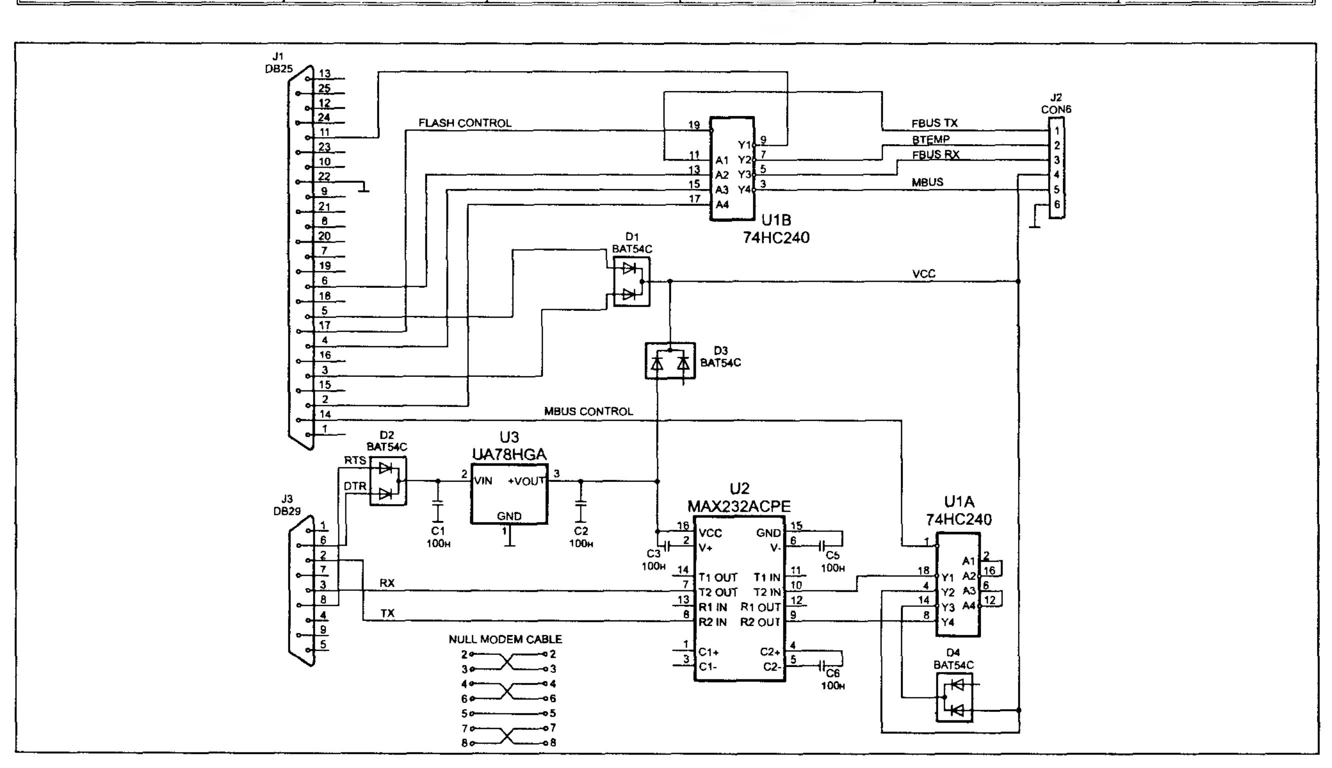


Рис. 8.17

Глава 9
Универсальные устройства для связи ПК и сотовых телефонов

Для связи ПК и телефонов используют как DATA-кабели, так и универсальные боксы*. Использование последних предпочтительнее, так как в совокупности они обходятся значительно дешевле комплекта DATA-кабелей (в каждом из которых имеются встроенные схемы конверторов интерфейсов — например, RS232—EMMI или USB—MBUS), подходящего к большинству моделей сотовых телефонов. В боксе сам преобразователь уже имеется, а телефоны подключаются к нему через простые переходники.

В этой главе описывается несколько видов универсальных боксов. Эти устройства достаточно просты, поэтому их можно изготовить самостоятельно.

* *Для программирования сотовых телефонов используются еще устройства, называемые «клипами» (clip) Они являются полностью автономными аппаратами, реализующими в себе функции и протоколы подключаемого интерфейса, и предназначены только для разблокировки мобильных телефонов.*

Универсальный бокс для подключения телефонов с интерфейсами SERIAL BUS и MBUS/CBUS к COM-порту ПК

Существует огромное количество схем DATA-кабелей и боксов для различных моделей телефонов, построенных на универсальных микросхемах MAX232 (Uп = 5 В) или MAX3232 (Uп = 3 В). Они представляют собой преобразователи уровней интерфейса RS232 в уровни ТТЛ, и наоборот.

На рис. 9.1 приведена принципиальная схема универсального бокса, позволяющая подключить телефоны с интерфейсом SERIAL и MBUS/CBUS к ПК.

Эта конструкция является наиболее удобной, так как позволяет оперативно переключать бокс в различные режимы работы, достаточно проста в изготовлении, имеет возможность добавления дополнительных функций и позволяет использовать готовые кабели-переходники, предназначенные для других боксов (**Griffinbox, Martechbox, Ufstornadobox, Unibox V5.0**).

Принцип работы универсального бокса

Основой конструкции является микросхема MAX232 — преобразователь уровней сигналов RS232 в уровни ТТЛ и наоборот. Как уже отмечалось выше, микросхема питается напряжением 5 В.

Эта микросхема состоит из четырех конверторов, два из которых преобразуют сигналы RS232 в ТТЛ, а два оставшихся — из ТТЛ в RS232.

Примечание. *Такой преобразователь необходим, так как размах сигналов RS232 на ПК —12 В, а на телефоне — около 3 В Если сигналы с выхода интерфейса RS232 подать напрямую на телефон, они могут вывести входные цепи его отладочного интерфейса из строя Уровни же сигналов, формируемые на системном соединителе телефона, недостаточны для подключения к компьютеру «напрямую»*

В предлагаемом устройстве используются только два конвертора.

Микросхема MAX232 в боксе используется в стандартном включении.

Емкость электролитических конденсаторов C6-C9, подключенных к выв. 1-6 конвертора, может находиться в пределах 1...10 мкФ.

Сигнал TX, формируемый на конт. 3 разъема RS232 компьютера, подается на вход конвертора, выв. 8 микросхемы. С выхода конвертора (выв. 9 IC1) сигнал ТТЛ-уровня подается на контакты соединителей J1, J2 и, уже как RX — на системный соединитель телефона.

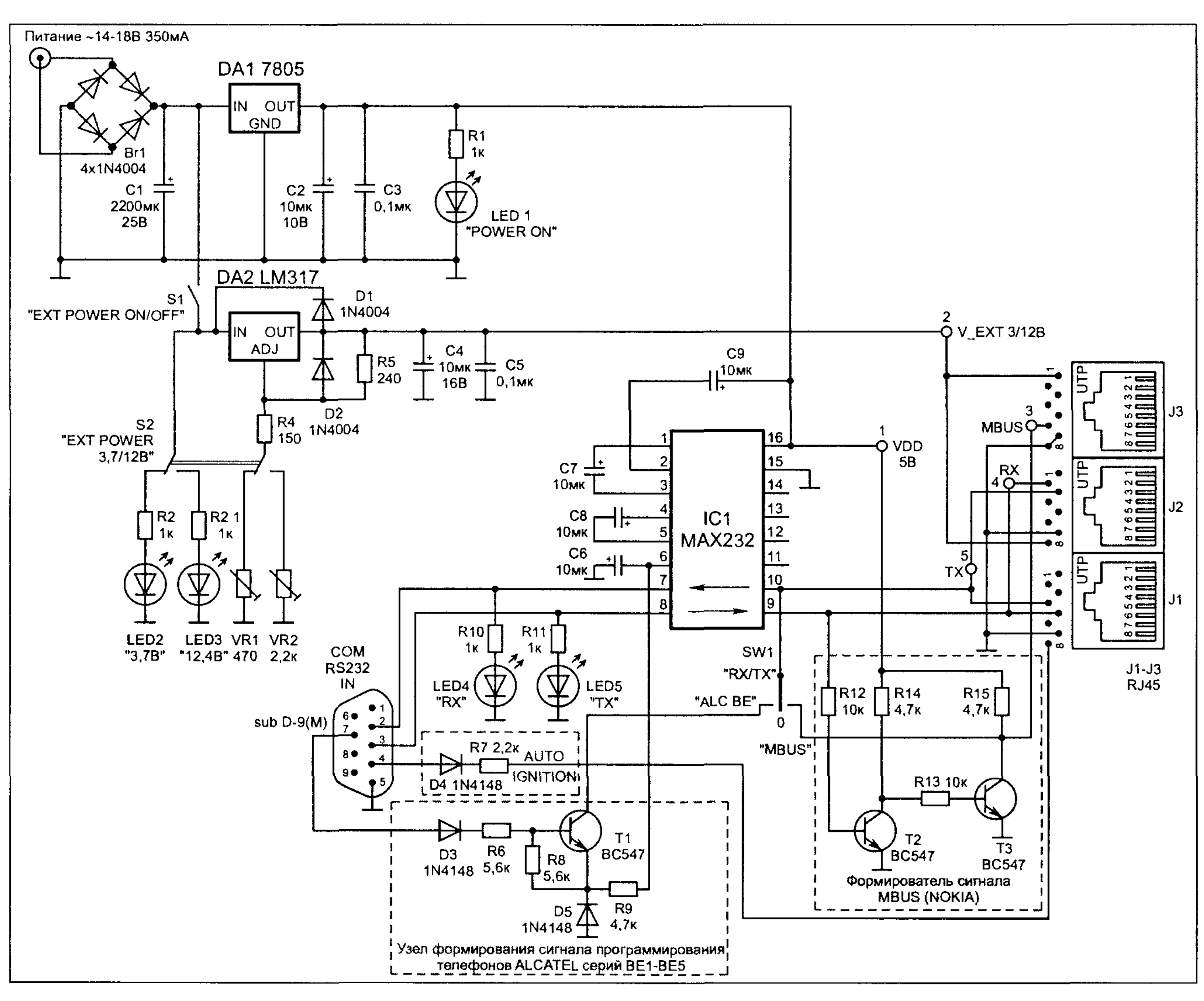


Рис. 9.1

Аналогично конвертируется сигнал TX, формируемый телефоном: с соединителей J1, J2 он поступает на выв. 10 IC1, снимается, уже как RX на выв. 7 микросхемы и, далее, подается на конт. 2 соединителя RS232.

Для контроля прохождения сигналов RX/TX к этим линиям подключены светодиоды LED4 и LED5. Их желательно использовать разного цвета свечения.

С конт. 4 соединителя RS232 через цепь VD4 R7 на конт. 8 соединителя J1, а затем на интерфейсный контакт телефона EXTERNAL POWER служащий для подключения зарядного устройства, поступает сигнал AUTO IGNITION. Этот сигнал активируется на ПК специальным программным обеспечением и используется, в основном, телефонами SIEMENS. Этим сигналам аппарат включается принудительно, без кратковременного нажатия на кнопку включения питания телефона. Этот сигнал также можно использовать для телефонов других производителей, если используется соответствующее программное обеспечение.

Узел, собранный на элементах: D3, D5, R6-R9, T1, используется для формирования служебного сигнала программирования телефонов ALCATEL серий BE1-BE5.

На элементах R12-R15, T2, T3 собран формирователь сигнала M2BUS, предназначенный для программирования телефонов NOKIA. Выход формирователя подключен к соединителю J3 бокса.

Переключатель SW1 служит для исключения взаимного влияния различных узлов схемы, предназначенных для программирования телефонов с разными интерфейсами, а также для переключения режимов работы бокса. Положение SW1 «ALC BE» соответствует режиму программирования телефонов ALCATEL серии BE, а положение SW1 «нейтраль» — программированию телефонов любых марок, использующих сигналы RX/TX. Позиция SW1 «MBUS» используется при программировании телефонов NOKIA.

Для питания микросхемы IC1 используется стабилизатор напряжения DA1 (5В). Наличие

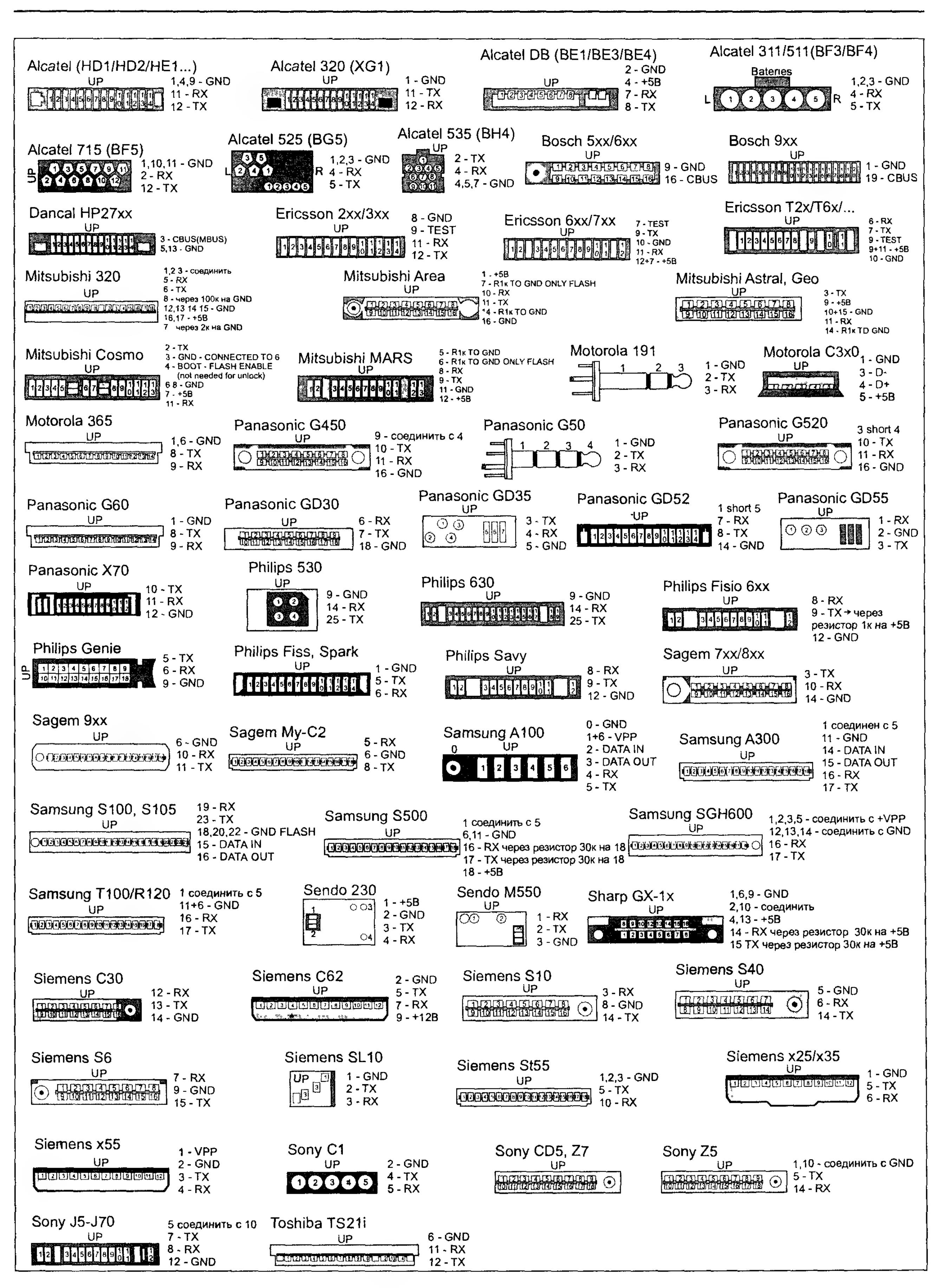

Alcatel (HD1/HD2/HE1...)
UP
1,4,9 - GND
11 - RX
12 - TX
Alcatel 320 (XG1)
UP
1 - GND
11 - TX
12 - RX
Alcatel DB (BE1/BE3/BE4)
UP
2 - GND
4 - +5B
7 - RX
8 - TX
Alcatel 311/511(BF3/BF4)
Bateries
L R
1,2,3 - GND
4 - RX
5 - TX
Alcatel 715 (BF5)
UP
1,10,11 - GND
2 - RX
12 - TX
Alcatel 525 (BG5)
L R
1,2,3 - GND
4 - RX
5 - TX
Alcatel 535 (BH4)
UP
2 - TX
4 - RX
4,5,7 - GND
Bosch 5xx/6xx
UP
9 - GND
16 - CBUS
Bosch 9xx
UP
1 - GND
19 - CBUS
Dancal HP27xx
UP
3 - CBUS(MBUS)
5,13 - GND
Ericsson 2xx/3xx
UP
8 - GND
9 - TEST
11 - RX
12 - TX
Ericsson 6xx/7xx
UP
7 - TEST
9 - TX
10 - GND
11 - RX
12+7 - +5B
Ericsson T2x/T6x/...
UP
6 - RX
7 - TX
9 - TEST
9+11 - +5B
10 - GND
Mitsubishi 320
UP
1,2 3 - соединить
5 - RX
6 - TX
8 - через 100к на GND
12,13 14 15 - GND
16,17 - +5B
7 через 2к на GND
Mitsubishi Area
UP
1 - +5B
7 - R1к TO GND ONLY FLASH
10 - RX
11 - TX
*4 - R1к TO GND
16 - GND
Mitsubishi Astral, Geo
UP
3 - TX
9 - +5B
10+15 - GND
11 - RX
14 - R1к TO GND
Mitsubishi Cosmo
UP
2 - TX
3 - GND - CONNECTED TO 6
4 - BOOT - FLASH ENABLE (not needed for unlock)
6 8 - GND
7 - +5B
11 - RX
Mitsubishi MARS
UP
5 - R1к TO GND
6 - R1к TO GND ONLY FLASH
8 - RX
9 - TX
11 - GND
12 - +5B
Motorola 191
1 2 3
1 - GND
2 - TX
3 - RX
Motorola C3x0
UP
1 - GND
3 - D-
4 - D+
5 - +5B
Motorola 365
UP
1,6 - GND
8 - TX
9 - RX
Panasonic G450
UP
9 - соединить с 4
10 - TX
11 - RX
16 - GND
Panasonic G50
1 2 3 4
1 - GND
2 - TX
3 - RX
Panasonic G520
UP
3 short 4
10 - TX
11 - RX
16 - GND
Panasonic G60
UP
1 - GND
8 - TX
9 - RX
Panasonic GD30
UP
6 - RX
7 - TX
18 - GND
Panasonic GD35
UP
3 - TX
4 - RX
5 - GND
Panasonic GD52
UP
1 short 5
7 - RX
8 - TX
14 - GND
Panasonic GD55
UP
1 - RX
2 - GND
3 - TX
Panasonic X70
UP
10 - TX
11 - RX
12 - GND
Philips 530
UP
9 - GND
14 - RX
25 - TX
Philips 630
UP
9 - GND
14 - RX
25 - TX
Philips Fisio 6xx
UP
8 - RX
9 - TX → через резистор 1к на +5B
12 - GND
Philips Genie
UP
5 - TX
6 - RX
9 - GND
Philips Fiss, Spark
UP
1 - GND
5 - TX
6 - RX
Philips Savy
UP
8 - RX
9 - TX
12 - GND
Sagem 7xx/8xx
UP
3 - TX
10 - RX
14 - GND
Sagem 9xx
UP
6 - GND
10 - RX
11 - TX
Sagem My-C2
UP
5 - RX
6 - GND
8 - TX
Samsung A100
0 UP
0 - GND
1+6 - VPP
2 - DATA IN
3 - DATA OUT
4 - RX
5 - TX
Samsung A300
UP
1 соединен с 5
11 - GND
14 - DATA IN
15 - DATA OUT
16 - RX
17 - TX
Samsung S100, S105
UP
19 - RX
23 - TX
18,20,22 - GND FLASH
15 - DATA IN
16 - DATA OUT
Samsung S500
UP
1 соединить с 5
6,11 - GND
16 - RX через резистор 30к на 18
17 - TX через резистор 30к на 18
18 - +5B
Samsung SGH600
UP
1,2,3,5 - соединить с +VPP
12,13,14 - соединить с GND
16 - RX
17 - TX
Samsung T100/R120
UP
1 соединить с 5
11+6 - GND
16 - RX
17 - TX
Sendo 230
1 - +5B
2 - GND
3 - TX
4 - RX
Sendo M550
UP
1 - RX
2 - TX
3 - GND
Sharp GX-1x
UP
1,6,9 - GND
2,10 - соединить
4,13 - +5B
14 - RX через резистор 30к на +5B
15 TX через резистор 30к на +5B
Siemens C30
UP
12 - RX
13 - TX
14 - GND
Siemens C62
UP
2 - GND
5 - TX
7 - RX
9 - +12B
Siemens S10
UP
3 - RX
8 - GND
14 - TX
Siemens S40
UP
5 - GND
6 - RX
14 - TX
Siemens S6
UP
7 - RX
9 - GND
15 - TX
Siemens SL10
UP
1 - GND
2 - TX
3 - RX
Siemens St55
UP
1,2,3 - GND
5 - TX
10 - RX
Siemens x25/x35
UP
1 - GND
5 - TX
6 - RX
Siemens x55
UP
1 - VPP
2 - GND
3 - TX
4 - RX
Sony C1
UP
2 - GND
4 - TX
5 - RX
Sony CD5, Z7
UP
Sony Z5
UP
1,10 - соединить с GND
5 - TX
14 - RX
Sony J5-J70
UP
5 соединить с 10
7 - TX
8 - RX
12 - GND
Toshiba TS21i
UP
6 - GND
11 - RX
12 - TX

Рис. 9.2

этого напряжения контролируется светодиодом LED1.

На микросхеме DA2, переключателе S2 и других элементах выполнен коммутируемый стабилизатор напряжения. В левом (по схеме) положении переключателя S2 он формирует напряжение 3,7 В для мобильных телефонов, а во втором — напряжение 12 В для программирования FLASH-памяти некоторых моделей аппаратов. Регулировка напряжений производится подстроечными резисторами VR1 и VR2. Наличие этих напряжений контролируется светодиодами LED2 и LED3. Выключатель S1 коммутирует включение стабилизатора DA2.

Бокс питается от битовой сети 220 В/50 Гц через AC/DC-адаптер с выходным напряжением 14...20 В и током не менее 350 мА.

Стабилизаторы DA1 и DA2 желательно установить на небольшие гребенчатые радиаторы с площадью около 30 см².

Для совместимости с кабелями-переходниками других типов боксов (как отмечалось выше — Griffinbox, Martechbox, Ufstornadobox и Unibox V5.0), в этом устройстве используются соединители J1-J3 типа RG45.

Назначение контактов соединителей J1-J3 приведено в таблице 9.1.

Наименование соединителя		№ конт	Назначение контакта	Используемые переходники
UTP 87654321	J1	1	+V_EXT	MARTECH UFS GRIFFIN
		2	NC	
		3	NC	
		4	TX	
		5	RX	
		6	NC	
		7	GROUND	
		8	AUTO_IGNITION	
	J2	1	NC	UNIBOX v5 0 UNIBOX
		2	RX	
		3	TX	
		4	NC	
		5	NC	
		6	NC	
		7	GROUND	
		8	+V_EXT	
	J3	1	+V_EXT	NOKIA MBUS GRIFFIN UFS
		2	NC	
		3	NC	
		4	NC	
		5	NC	
		6	MBUS	
		7	GROUND	
		8	GROUND	

Кабели-переходники к этому боксу можно изготовить самостоятельно, для этого необходимы ответные части системных соединителей соответствующих типов телефонов, а также вилки RG45. На рис. 9.2 показаны системные соединители, а также назначение их контактов для некоторых моделей телефонов.

Примечание. *При самостоятельном изготовлении кабелей-переходников следует учесть, что сигналы TX/RX на соединителях J1, J2 обозначены как на системных соединителях телефонов Например, если на соединителе телефона сигнал обозначен как TX (аналогично и на конт 2 J1 и конт 3 J2), а уже на выв 10 микросхемы IC1 (и далее — до разъема RS232) он обозначен, как RX Все сказанное в полной мере относится и к USB-боксам (см ниже)*

Универсальные боксы для подключения телефонов с интерфейсами SERIAL BUS и MBUS/CBUS к USB-порту ПК

Универсальные боксы с USB-интерфейсом, в отличие от предыдущего (см. рис. 9.1), предназначены для программирования телефонов с интерфейсами SERIAL BUS и MBUS/CBUS.

На сегодняшний момент существуют несколько распространенных схем USB UNIBOX. Они построены на разных микросхемах, но выполняют одну и ту же функцию: конвертируют сигналы с уровнями интерфейса USB в сигналы с уровнями интерфейса RS232 (с ТТЛ-выходом). Их еще называют мостами «USB-to-RS232 BRIDGE». При подключении такого бокса к компьютеру требуется установить драйвер для конкретного типа микросхемы, используемой в качестве конвертора. После установки такого драйвера в закладке УСТРОЙСТВА появляется дополнительный СОМ-порт. На рис. 9.3 показано окно, где этот порт обозначен как COM 4. Для работы программного обеспечения при разблокировке и флэширования мобильных телефонов в настройках должна быть возможность выбора этого СОМ-порта.

Микросхема преобразователя эмулирует все сигналы, включая DSR, DCD и CTS.

Первая схема (см. рис. 9.4) универсального бокса USB построена на микросхеме FT232BM фирмы FTDI CHIP. Большинство узлов (питания и др.) аналогичны схеме, показанной на рис. 9.1. Основное отличие — другой тип микросхемы (FT232BM). Питание этой микросхемы осуществляется от USB-порта ПК, но для питания мобильного телефона и формирования напряжения

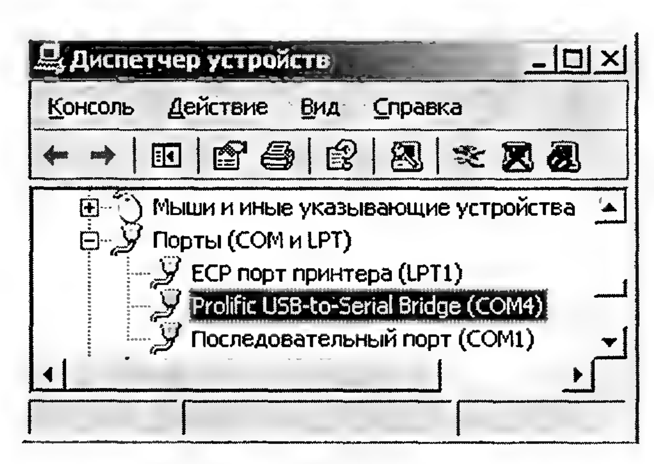


Рис. 9.3

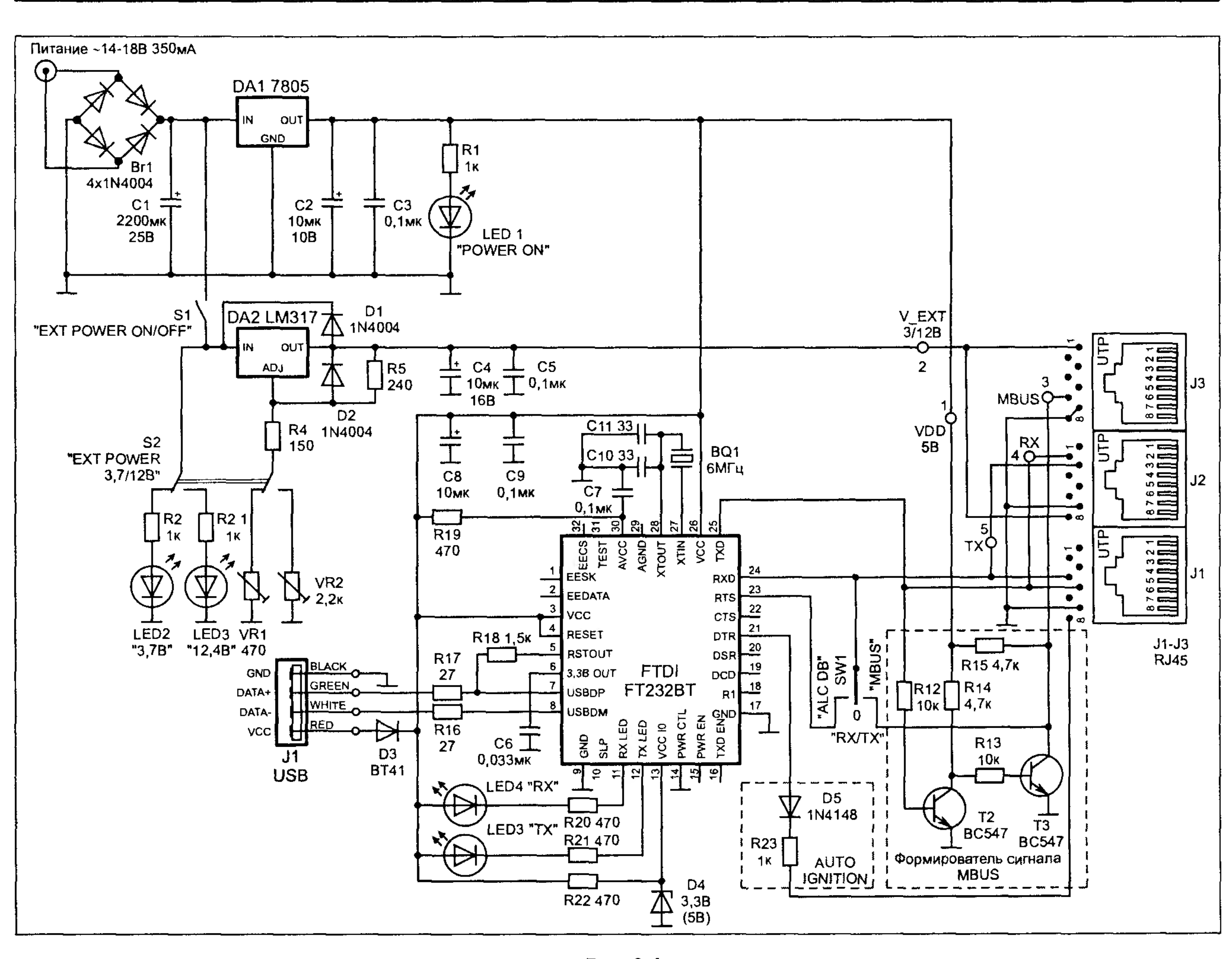


Рис. 9.4

программирования 12 В используется отдельный стабилизатор DA 2 типа LM317 (схема аналогична .рис. 9.1). При изготовлении данного бокса следует учесть, что эта микросхема выполнена в корпусе QFP.

Еще одна похожая схема (см. рис. 9.5) построена на микросхеме Prolific PL2303. На базе этой микросхемы собраны 99% китайских DATA-кабелей, реализуемых на российском рынке. Микросхема PL2303 выполнена в 28-выводном корпусе SSOP, что затрудняет сборку данной конструкции на макетной плате. Однако, чтобы обойти эту проблему, можно в качестве готового узла можно использовать «начинку» от любого китайского USB DATA-кабеля.

Можно еще порекомендовать еще одну схему USB-бокса, выполненного на основе микросхемы CP2101. Его принципиальная схема показана на рис. 9.6.

Рис. 9.5

Рис. 9.6

Содержание